2/2023

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

46. Jahrgang
ISSN 0137-7767
14,00 Euro



Europäische Entwicklungen (Teil 2)

■ „Bei der Durchsetzung des Grundrechts auf Datenschutz steht man zum großen Teil einfach vor verschlossenen Türen" ■ Ausgewählte Rechtsetzungsinitiativen der Europäischen Union im Zeitalter der digitalen Revolution ■ Überlegungen zu einer datenschutzkonformen europäischen Forschungsregulierung ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Foto: Pixabay..com

Dienstag, 01.08.2023
Redaktionsschluss DANA 3/2023
„Whistleblowing"

Sonntag, 10.09.2023
Vorstandssitzung der DVD
Kiel

Montag, 11.09.2023
Sommerakademie des ULD Schleswig-Holstein
Kiel

Freitag-Montag, 01.-04.09.2023
„Freedom not Fear"-Konferenz
Brüssel

Mittwoch-Freitag, 04.-06.10.2023
Jahrestagung Forum Privatheit „Data Sharing – Datenkapitalismus by Default?"
Berlin

Mittwoch-Freitag, 18.-20.10.2023
BvD-Herbstkonferenz & Behördentag
München

Mittwoch, 01.11.2023
Redaktionsschluss DANA 4/2023
„Internet of Things"

Samstag, 11.11.2023
Vorstandssitzung der DVD
Bonn

Sonntag, 12.11.2023
Mitgliederversammlung der DVD
Bonn

DANA
Datenschutz Nachrichten
ISSN 0137-7767
46. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert und Achim Klabunde
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Dr.-Mack-Straße 83
90762 Fürth
www.onlineprinters.de
Tel. +49 (0) 9161 6209800
Fax +49 (0) 9161 8989 2000

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (inkl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Nach einem Jahr kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Pixabay
Frans Jozef Valenta
Titel: iStock – Renato Arap

Editorial

Vor fünf Jahren wurde die Datenschutz-Grundverordnung vollständig anwendbar. Bereits am ersten Tag reichte die von Max Schrems gegründete Organisation noyb (none of your business) mehrere Beschwerden bezüglich der Datenverarbeitung durch die Dienste der inzwischen in Meta umbenannten Firma ein: Facebook, WhatsApp, Instagram. Die Bearbeitung dieser und anderer Beschwerden ist immer noch nicht vollständig abgeschlossen. Im Interview schildert Max Schrems die Erfahrungen mit der Durchsetzung des Datenschutzrechts durch die irische und andere Datenschutzaufsichtsbehörden. Auch die Europäische Kommission hat die Defizite erkannt und bereitet jetzt einen Vorschlag zur Verbesserung der Verfahren vor. Max Schrems hat allerdings Zweifel, ob der Ansatz der Kommission hinreichend ist.

Die bereits in der letzten DANA-Ausgabe betrachteten Gesetzgebungsverfahren im Rahmen der EU-Digitalstrategie gehen weiter. DSA (Gesetz über digitale Dienste), DMA (Gesetz über digitale Märkte) und DGA (Daten-Governance-Rechtsakt) sind beschlossen und jetzt auch vollständig anwendbar. Die Gesetzgebungsverfahren zu DA (Data Act), EHDS (European Health Data Space) und AIA (AI Act) gehen voran, sodass eine Verabschiedung vor der nächsten Wahl des Europäischen Parlaments in einem Jahr noch möglich erscheint. Axel Freiherr von dem Bussche und Alexander Schmalenberger analysieren das Zusammenwirken dieser Rechtsakte mit der Datenschutz-Grundverordnung. Die in allen Regelungen enthaltene deklaratorische Klausel, dass die DSGVO „unberührt" bleibe, kann in dieser Simplizität nicht überzeugen.

Der Europäische Raum für Gesundheitsdaten (EGDR, EHDS) soll unter anderem auch die Forschung mit solchen Daten fördern. Thilo Weichert betrachtet die Vorhaben zur verstärkten Nutzung von personenbezogenen Daten für Forschungszwecke in größerer Breite und schließt einen Paradigmenwechsel zu mehr Nutzung solcher Daten grundsätzlich nicht aus, findet allerdings erhebliche Lücken beim notwendigen Grundrechtsschutz.

Während der europäische Gesetzgeber mit den neuen Digitalgesetzen vorangeht, scheint dies nicht für die ePrivacy-Verordnung zu gelten. Die derzeitige schwedische Ratspräsidentschaft zeigt keinerlei Interesse daran diese Verhandlungen voranzutreiben. Achim Klabunde schreibt über Warnungen der Berichterstatterin des EP, Birgit Sippel (SPD), dass durch ein Scheitern des Gesetzgebungsverfahrens die Chance auf einen EU-weit einheitlichen Schutz des Kommunikationsgeheimnisses vertan werden könnte.

Auf einen kurzen Rückblick auf die BigBrotherAwards 2023 von Heinz Alenfelder und einen ebenfalls kurzen Artikel zum Einsatz der Polizeisoftware hessenDATA von Sakyi Mannah folgen wie in jeder DANA-Ausgabe Pressemitteilungen, offene Briefe, die Datenschutznachrichten, Meldungen zur Rechtsprechung und Buchbesprechungen.

Wir wünschen Ihnen und Euch eine angenehme und anregende Lektüre.

Autorinnen und Autoren dieser Ausgabe:

Heinz Alenfelder
Vorstandsmitglied der DVD, Köln,
alenfelder@datenschutzverein.de

Dr. Axel Freiherr von dem Bussche
Fachanwalt für Informationstechnologierecht, Taylor Wessing Partnerschaftsgesellschaft mbB, Hamburg,
a.bussche@taylorwessing.com

Achim Klabunde
Vorstandsmitglied der DVD, Bonn,
klabunde@datenschutzverein.de

Sakyi Mannah
Wissenschaftlicher Mitarbeiter des Selbstregulierung Informationswirtschaft e.V., Berlin, smannah@sriw.de

Alexander Schmalenberger
Rechtsanwalt / Knowledge Lawyer, Taylor Wessing Partnerschaftsgesellschaft mbB, Hamburg,
a.schmalenberger@taylorwessing.com

Maximilian „Max" Schrems
Vorstandsvorsitzender noyb,
info@noyb.eu

Dr. Thilo Weichert
Vorstandsmitglied der DVD, Netzwerk Datenschutzexpertise, Kiel,
weichert@datenschutzverein.de

„Bei der Durchsetzung des Grundrechts auf Datenschutz steht man zum großen Teil einfach vor verschlossenen Türen."

(Das Interview mit Max Schrems führte DVD-Vorstand Achim Klabunde.)

Max Schrems ist Gründer und Vorsitzender des Vereins noyb[1] (none of your business), der sich für die juristische und politische Durchsetzung der Rechte von Betroffenen nach der DSGVO einsetzt. Max Schrems wurde international als Kläger bekannt in Verfahren, die letztlich zur Annullierung der Entscheidungen der Europäischen Kommission durch den EuGH führten, mit denen die Kommission die US-Verfahren Safe Harbor bzw. Privacy Shield als angemessen eingestuft hatte.

Gerade ist es fünf Jahre her, dass die DSGVO voll anwendbar wurde. noyb hat sich ja von Anfang an mit der Durchsetzung von Datenschutzrechten befasst. Wie lange gibt es noyb eigentlich jetzt?

Uns gibt es operational auch seit fünf Jahren, weil wir praktisch richtig mit der Anwendbarkeit der DSGVO angefangen haben.

Wie wichtig war eigentlich die irische Datenschutzbehörde für die Entstehung von noyb?

Die Erfahrungen mit der irischen Datenschutzbehörde vor der DSGVO haben schon eine Rolle gespielt. Das war aber nicht der wesentliche Faktor. Mit der Verabschiedung der DSGVO war es schon so, dass wir uns dachten „Also, schauen wir mal, ob die Datenschutz-Aufsichtsbehörden dann wirklich etwas tun." Und es braucht halt jemanden, der da vielleicht ein bisschen hinterher ist. Und ich muss ehrlich sagen, wir haben deutlich unterschätzt, wie wenig die Behörden jetzt wirklich aktiv geworden sind. Der alte Ansatz aus der Zeit der Richtlinie, nach dem Motto „Reden wir mal darüber und machen wir mal irgendein Paper und so weiter" ist halt noch immer sehr, sehr stark. Und dieser Kulturwandel zu einer Durchsetzungs-Organisation hat halt nicht wirklich stattgefunden, das merkt man schon sehr stark. Also ich glaube, dass es noyb aktuell mehr braucht als ursprünglich gedacht.

noyb hat gleich am ersten Tag der Anwendbarkeit der DSGVO mehrere Beschwerden eingereicht. In Irland, in Luxemburg, in Frankreich, in Österreich sicher auch. Nach fünf Jahren sollten die ja alle vollständig bearbeitet sein. Wie ist denn da der Stand?

Ja, also der Stand ist ganz interessant. Ein Fall war in Frankreich, und das war Google, und da hat die französische Behörde direkt entschieden. Das war mal in neun Monaten entschieden. Zwar auch nicht ganz, aber zumindest im Kern. Auch mit einer Strafe von 50 Millionen Euro. Die anderen Fälle sind nach Irland gegangen und da ist einfach jahrelang nichts entschieden worden. Da werden Berichte geschrieben und wieder Berichte geschrieben und die Akten werden dicker und dicker und dicker.

Eine unserer Beschwerden betrifft die Rechtsgrundlagen der Datenverarbeitung von Facebook. Also, die probieren halt statt der ausdrücklichen Einwilligung zur Verarbeitung eine Einwilligungsklausel in den Nutzungsvertrag zu schreiben und dann zu sagen: „Naja, wenn die Einwilligung im Vertrag steht, dann ist es vertraglich notwendig und dann gilt nicht mehr Art. 6 Abs. 1 lit. a, sondern Art. 6 Abs. 1 lit. b der DSGVO." Das war so die Idee. Zu diesem Thema hat ja der EDSA schon Anfang 2019 die Leitlinien[2] über die Verarbeitung von personenbezogenen Daten aufgrund von Verträgen beschlossen, und da war eigentlich dann schon klar, dass europaweit eigentlich diese Sicht herrscht, dass das Vorgehen von Facebook nicht geht. Die irische Behörde hatte ja probiert in diese Leitlinien hinein zu reklamieren, dass soziale Netzwerke für Werbung das tun können sollen. Natürlich hat die irische Behörde gesagt, dass ihre Forderung gar nicht spezifisch sei zu dem Fall, der gerade bei ihnen liegt.

Als die Leitlinien beschlossen waren, hat die irische Behörde dann an den EDSA geschrieben, dass bitte diese Leitlinien nicht veröffentlicht werden sollen, weil sie ja jetzt unmittelbar einen Fall haben und der ja bald entschieden wird. Und die Entscheidung war dann vier Jahre später.

An diesem Fall sieht man halt, wie mit einem Draft von einem Draft von einem Report, der dann wieder irgendwie beantwortet wird und zirkuliert wird, Verfahren wirklich endlos verzögert werden. Und man muss sagen, dass wir in Irland ja in der Zwischenzeit schon ein Gerichtsverfahren gegen die irische Behörde angestrengt hatten, dass die da überhaupt entscheiden. Und selbst das Gerichtsverfahren ist zwei Jahre lang verzögert worden, bis wir überhaupt mal vor einem Richter standen, der sich anhörte, dass das behördliche Beschwerdeverfahren verzögert ist. Also am Ende merkt man, dass man einfach durch Papiere produzieren und sie im Kreis zu schicken halt unaufhaltsame Ergebnisse zwar nicht verhindern kann, sie aber trotzdem sehr lange herauszögern kann. Und da sieht man halt, dass auch die Verfahren dann nicht so gut funktionieren.

Die Beschwerden von noyb bezüglich der verschiedenen Dienste von Meta (damals noch Facebook) waren auch die Grundlage für die verbindlichen Entscheidungen des EDSA gemäß Art. 65 DSGVO[3].

Wir haben von Anfang an die Meinung vertreten, dass eine Vertragsklausel die Anforderungen der DSGVO an eine Einwilligung erfüllen muss, weil es für die Einwilligung ja egal ist, ob die Einwilligung in den AGB drinsteht oder woanders. Der Natur nach ist das eine Einwilligung, und es kann keinen Unterschied machen, wenn es auf einem anderen Papier draufsteht. Der EDSA hat die Möglichkeit der Anwendung von Art. 6 Abs. 1 lit. b DSGVO im Fall von Facebook diskutiert und hat gefunden, dass das so nicht geht und hat damit die Vertragsklausel nicht als gültige Einwilligung betrachtet.

Auf unsere ursprüngliche Beschwerde, dass diese Vertragsklausel keine Einwilligung und deswegen ungültig sei, hatten die Iren gesagt, eben weil es die Definition der Einwilligung nicht erfüllt, weil sie nicht freiwillig ist und so weiter, kann es ja gar keine Einwilligung sein, deswegen muss es ein Vertrag sein. Also wir haben das Ganze halt umgekehrt aufgezäumt. Wir haben dann, nachdem uns klar geworden ist, dass Facebook beinhart auf Art. 6 Abs. 1 lit. b DSGVO als Rechtsgrundlage besteht, eine Liste gemacht von, je nach Dienst, bis zu neun oder zehn verschiedenen Zwecken, für die aufgrund des Vertrages einfach keine Rechtsgrundlage besteht. Wir haben dann gesagt, gut, dann diskutieren wir nicht, was für eine Rechtsgrundlage das ist, sondern probieren wir den Fall halt anhand der Zwecke aufzuziehen und zu sagen, gut, diese fünf, sechs, sieben, acht Zwecke sind auf jeden Fall nicht gedeckt, egal, was ihr da jetzt einordnet. Und da ist es interessant, dass wir eigentlich von diesen Zwecken nur zu einem halben überhaupt eine Entscheidung bekommen haben.

Also wir haben da zum Beispiel gesagt, die Daten dürfen jetzt auch nicht weitergegeben werden an verbundene Unternehmen oder die dürfen jetzt auch nicht für die Personalisierung vom Content verwendet werden und so weiter. Also gibt es alle möglichen Zwecke, die da drinnen sind und der EDSA hat dann statt zu dem was wir beantragt haben, nämlich zur Werbung, zu entscheiden, seine Entscheidung beschränkt auf die Verwendung der Daten für behavioral advertisement, also verhaltensbasierte Werbung. Das war aber nicht unser Antrag. Unser Antrag war, die Daten dürfen generell nicht für Werbung verwendet werden. Und keiner weiß eigentlich, warum der EDSA seine Entscheidung auf behavioral advertisement limitiert hat, und keiner weiß auch, warum die Anträge bezüglich der anderen zehn Zwecke eigentlich nie bearbeitet worden sind.

Die Österreicher sagen zum Beispiel, das liegt jetzt noch vor der irischen Behörde und natürlich sind die Anträge rechtsgültig eingebracht und die müssen entschieden werden. Und die irische Behörde sagt wiederum, die Anträge hätten sie nicht bearbeitet, weil sie gar nicht in der ursprünglichen Beschwerde enthalten waren. Das heißt, die Behörden streiten schon mal, was überhaupt der Gegenstand der Beschwerde ist, und das viereinhalb Jahre später. Für uns ist das die Schwierigkeit: Egal, vor welches Gericht wir gehen, sagt halt jede beklagte Behörde, die andere Behörde hat etwas falsch gemacht. Also, in Österreich sagen sie, sie hätten die Beschwerde ganz vorbildlich nach Irland geschickt. Und was können sie dafür, dass die Iren jetzt nichts tun?

Und die Iren sagen, das ist überhaupt nie von Österreich zu uns gekommen, weil sie ignorieren, dass das überhaupt ein Teil des Verfahrens ist. Und damit ist man dann als Beschwerdeführer strukturell am Ende des Rechtswegs angekommen.

An diesem Beispiel des Facebook-Verfahrens haben wir die fehlende Rechtsgrundlage der Verarbeitung für neun verschiedene Zwecke bemängelt, und zu einem halben Zweck ist entschieden worden, und das nach viereinhalb Jahren. Das alles passiert in einem Fall, der eigentlich sehr viel Aufmerksamkeit bekommen hat, dann sieht man deutlich, dass es massive Probleme mit der Durchsetzung der DSGVO hat.

Ja. Also man fragt sich, ist das mehr Kafka oder mehr Joyce?

Also ich habe irgendwann mal angefangen Kafka zu lesen, weil alle so oft darauf referenziert haben und ich muss ehrlich sagen, was wir die letzten fünf Jahre erlebt haben, da ist Kafka also wirklich harmlos dagegen. Wir haben Fälle, also ganz banale Sachen, wir haben Fälle, wo die Iren und die Franzosen jetzt dreimal schon im Kreis streiten, wer eigentlich zuständig ist für Google. Jeder sagt, der andere ist zuständig. Dann haben wir in Polen zum Beispiel, wenn du Akteneinsicht nehmen willst, sagen die, nein, das geht nur physisch bei der polnischen Datenschutzbehörde in Warschau. Das heißt, du musst dann dort irgendwo aus Europa nach Warschau fahren oder fliegen.

Und dann gibt es dort keinen Kopierer, sondern du musst mit deinem Handy Fotos machen von den Akten. Du kriegst aber pro Akte nur begrenzte Zeit, etwa 30 Minuten. In Irland haben wir immer wieder solche Situationen. In Irland streiten wir über jedes blöde Dokument, wo es heißt, ja, wir hätten alle Unterlagen bekommen, aber dann sehen wir in irgendeiner Fußnote, dass wieder irgendein Dokument referenziert worden ist, das wir nicht bekommen haben. Dann muss man dem wieder hinterherlaufen, und man kriegt es dann nach drei Monaten, und in dem Dokument stehen wieder fünf andere Dokumente, die man auch noch nicht bekommen hat. Die Österreicher sagen dann, die Iren geben es uns nicht, oder die Deutschen sagen dann das gleiche, die Iren sagen, ja wir geben es euch gar nicht, weil es schon Argumente gegeben hat, dass sie das aus irgendwelchen Datenschutzgründen nicht weitergeben können. Prinzipiell stempeln die Unternehmen alle Akten, wirklich jedes E-Mail, als Betriebs- und Geschäftsgeheimnis. Selbst eine E-Mail, in der nur steht „Entschuldigung, wir bringen die Antwort erst eine Woche später ein." wird dann als Betriebs- und Geschäftsgeheimnis eingestuft.

Und es wird wirklich auf allen Ebenen versucht irgendwie diese Fälle loszuwerden, Da sehen wir halt auch einen sehr großen Trend von den Behörden. Ich verstehe natürlich die Motivation. Es gibt ein extrem hohes Beschwerdeaufkommen, weil sich einfach auch wirklich wenig an das Gesetz gehalten wird, und die Behörden probieren dann zu einem großen Teil diese Beschwerden irgendwie nicht bearbeiten zu müssen. Der extremste Fall ist aktuell Frankreich, wo die Behörde einfach prinzipiell die Meinung vertritt, sie müsse Beschwerden überhaupt nicht bearbeiten.

Das sei eher so eine Art Petition oder so eine Art Informationsschreiben an die Behörde.

Leider sehen wir Ähnliches dann auch bei den Gerichten. Eine Durchsetzungsoption der DSGVO sind ja Zivilgerichte und dort sieht man auch, dass sich viele Richter einfach nicht mit der DSGVO beschäftigen wollen. Es ist ein Gesetz, das sie noch nie gesehen haben, was kompliziert ist und dann probiert man irgendeinen Grund zu finden, um den Fall abzuweisen.

Damit steht man wirklich mit diesem Grundrecht auf Datenschutz zum großen Teil einfach vor verschlossenen Türen. Also jeder sagt: „Bitte, ich verstehe, eh ganz wichtig, Grundrechte. Aber bitte nicht bei mir." Und das ist schon sehr extrem.

Dem EuGH liegen ja jetzt zwei Fälle vor, an denen ihr auch beteiligt wart.

Einmal geht da es um den Fall, wo der österreichische Richter gesagt hat, Datenverlust ist doch kein Schaden. Ja, in dem Fall war es noch ein bisschen differenzierter, weil die österreichische Post die wahrscheinliche politische Ausrichtung ihrer Kunden berechnet hat. Und dem Betroffenen ist sozusagen berechnet worden, dass er der rechtsextremen FPÖ nahe wäre. Allerdings war der auf der österreichischen Robinson-Liste drauf und die Post sagt, soweit sie das nachvollziehen kann, hat sie diese Daten nie an jemand anderen weitergegeben, sondern es war sozusagen nur bei ihnen lokal gespeichert. Und sie glauben, dass sie es nie jemandem weitergegeben haben. Ob es weitergegeben worden ist oder nicht, könne man heutzutage einfach nicht mehr feststellen, also nach 20 Jahren weiß man es nicht mehr, wann das wo weitergegeben worden ist oder nicht. Es gibt also einfach kein Beweisergebnis zur Frage der Weitergabe.

So, und jetzt war die Frage, ob allein diese Berechnung über ihn, die ihn halt ein bisschen empört hat, weil das halt politisch doch ein bisschen extrem ist, ob das schon zum Schadenersatz reicht. Und da ist interessant, und da sieht man auch die Struktur, mit der wir sehr viel beschäftigt sind. Es hat ja in Deutschland diese Theorie von einer Erheblichkeitsschwelle gegeben für Schadenersatz und das kommt aus dem deutschen Grundgesetz und hat nach dem deutschen BDSG auch Sinn gemacht, weil man ja gesagt hat, es kann ja nicht das allgemeine Persönlichkeitsrecht nach dem Grundgesetz und der Schadenersatz nach dem BDSG verschieden sein. Da hat es Sinn gemacht.

Jetzt hat man probiert diese Rechtsprechung auf die DSGVO zu übertragen. Und in der DSGVO gibt es aber überhaupt kein Sterbenswörtchen zu einer erheblichen Verletzung. Da steht einfach nur immaterieller Schaden. Und das ist interessant, weil wir in anderen europäischen Rechtsgebieten, also zum Beispiel, mit dem ich es ganz gern vergleiche, der Pauschalreisenrichtlinie, ausdrücklich die Bedingung haben, dass ich eine erhebliche Trübung meiner Urlaubsfreuden haben muss. Und da kriegen Leute halt 500 Euro, weil statt einem Sandstrand ein Kieselstrand ist. Und das ist anscheinend ein emotionaler Schaden, der dann ein paar hundert Euro wert ist.

Gleichzeitig wird aber jetzt gesagt – und da gibt es eine sehr sinistre Formulierung, die der österreichische OGH vorgelegt hat – danach sei die bloße Konsequenz oder Rechtsbruch kein ersatzfähiger Schaden. Also sozusagen allein, dass jemand anderer ein Gesetz bricht, ist ja noch kein Schaden. Wenn du aber diese Formulierung nimmst, sozusagen der typische Schaden von einer zum Beispiel Auskunftsrechtsverletzung oder von einer Nichtlöschung oder von falschen Daten, dann ist das per Definition der typische Schaden. Also du kannst ja praktisch, wenn du sagst, der typische Schaden von einer Körperverletzung ist nicht ersatzfähig, dann hast du praktisch nie wieder einen Schaden ersetzt bekommen bei einer Körperverletzung. Und mit so einer Definition, die da versucht wird zu verwenden, ist es relativ leicht dann für nationale Richter zu sagen: „Naja, das war ja einfach nur ein ganz normaler Data Breach, da sind nur ganz normal 10 Millionen Daten abhandengekommen und dementsprechend ist es nicht schadenersatzfähig, weil ja das im Prinzip genau das gleiche ist."

Man muss auch rechnen, einfach die Kosten von so einem Gerichtsverfahren. Also eine Klage kostet bei uns aktuell je nach Land so im Schnitt etwa 5000 Euro. Darunter kriegst du praktisch niemanden, der vor irgendein Gericht geht. Damit klingt es zwar gut, dass die Behörde entscheiden muss und wenn die nicht innerhalb von drei Monaten mir sagt, was sie da getan hat, dann kann ich ja vor Gericht ziehen, aber kein Mensch zieht für 5000 Euro vor Gericht, weil das Einzige, was du davon kriegst, ist die Information, dass sie nichts gemacht haben.

Und da hat man schon eine Situation, wo das sich in der Theorie alles super anhört. Man kann dann mal eine Beschwerde einbringen und das ist kostenfrei und so weiter. Aber wenn dann einfach die Behörde strukturell nicht darauf reagiert?

In Irland hat es Zahlen gegeben von bis zu 10.000 Beschwerden im Jahr, inzwischen sagt die Behörde, es sind nur 3.000 Beschwerden, weil man einfach ein bisschen umdefiniert hat, was eine Beschwerde ist. Aber man hat halt, was weiß ich, 10 Entscheidungen im Jahr. Dann hat man halt jenseits dieser Entscheidungen 99 Prozent aller Beschwerden, die zu keiner Entscheidung führen. Und dann kann ich zwar theoretisch in Irland vor den High Court gehen, aber das kostet in Irland bis zu 100.000 Euro, so eine Klage. Geschweige denn, dass ich überhaupt einen Anwalt finde, der mich verträte dafür, weil das auch sehr schwierig ist überhaupt Anwälte zu finden, die „pro Datenschutz" vertreten, weil praktisch alle auf der anderen Seite ihr Geld machen, dann hat man schon strukturelle Situationen, wo eigentlich die Durchsetzung dieser Rechte vollkommen fiktiv ist.

Nun ist es ein sehr spezieller Fall.

Ich denke schon, dass auch andere Datenschutzbehörden das Recht nicht so anwenden, wie man das eigentlich erwartet, nachdem der Gesetzgeber es beschlossen hat. Ja, also ich glaube, dass wir jetzt nach fünf Jahren eine Situation haben, wo die Exekutive und teilweise auch die Judikative schlichtweg den Gesetzgeber ignorieren. Ich denke, es ist schon sehr klar gewesen, dass die Idee des Gesetzgebers war, dass Datenschutz jetzt mit der DSGVO ordentlich durchgesetzt wird. Und man muss auch sagen, es waren über 90 Prozent,

die im EU-Parlament dafür gestimmt haben, es waren alle Mitgliedsstaaten dafür, bis auf Österreich, weil wir es irgendwie noch strenger haben wollten. Also dieses Gesetz hat demokratisch eine extrem große Legitimierung.

Und es hat Teile der Industrie oder teilweise auch sozusagen aus der Lehre und so weiter schon zusammengebracht fünf Jahre lang dieses Gesetz so zu bombardieren und so zu zerlöchern und so zu hinterfragen, dass innerhalb der Datenschutz-Bubble schon oft so das Gefühl ist: „Naja, also so ganz ernst kann man das ja nicht nehmen und so ganz voll kann man das ja nicht durchsetzen."

Das merken wir jetzt schon sehr stark, auch wenn wir mit Datenschutzbehörden sprechen.

Ich kann das jetzt nicht direkt zitieren, aber da gibt es Fälle, wo dir einfach Leute von den Behörden sagen „Ja, das wäre ja lustig, wenn wir das mal alles durchsetzen." Und dann stellt man sich schon die Frage, für was wir diese Behörden haben, für was wir diese Grundrechte haben. Und wir kriegen das auch in E-Mails sehr stark. Wir kriegen echt viele E-Mails, wo es dann heißt „Die sind alle korrupt und die machen eh nichts und die sind vollkommen nutzlos und so weiter." Natürlich gibt es halt einen gewissen Teil von Leuten, die sagen „Die Behörde hat mir voll toll geholfen und hat das super gemacht." Die muss man aber mit der Lupe suchen. Ich glaube, dass da oft jetzt einfach der Kulturwandel gefehlt hat. Also gar nicht jetzt irgendwie Bösartigkeit oder so was, sondern es ist ein Unterschied, wenn man eine Aufsichtsbehörde ist, die ein paar Guidelines macht und eine Konferenz und ein bisschen da herumtut, oder ob man halt eine wirkliche Durchsetzungsbehörde ist.

Ich glaube es ist schwierig zu verstehen, dass jeder Falschparker wahrscheinlicher eine Strafe bekommt als jemand, der Millionen Datensätze veruntreut. Das sehe ich auch sehr stark bei Konferenzen. Ich bin ja sehr stark auch bei Unternehmenskonferenzen als Speaker oder Vortragender. Und da sind die Leute inzwischen schon sehr klar und abgebrüht und sagen: „Die Realität ist, da wird nichts durchgesetzt, da wird es keine Konsequenz geben." Und auch oft sind – glaube ich – die Datenschutzbeauftragten frustriert, weil die halt sagen: „Ich sage meinem Chef, das ist eigentlich nicht erlaubt, aber die Antwort ist, es gibt eh keine Konsequenz." Und jetzt sind wir halt dann wieder auf dem Status, den wir gehabt haben bei der alten Richtlinie. Dass es zwar theoretisch dasteht, aber dann einfach faktisch nicht gemacht wird. Und da haben wir schon ein Rechtsstaatlichkeitsdemokratie-Problem, wirklich, weil, wenn wir in einem demokratischen Prozess entscheiden, dass es die Strafen gibt, – die für mich auch teilweise zu hoch sind und so weiter, das kann man alles diskutieren – aber am Ende gibt es eine demokratische Entscheidung und die wird aber einfach nicht durchgesetzt oder ignoriert, dann haben wir schon ein bisschen ein Rechtsstaatsproblem. Also ein bisschen ein großes.

Auf diese Beobachtungen hat ja nun die Europäische Kommission mit einer Initiative reagiert, zur Verbesserung der Verfahren zur Durchsetzung der DSGVO. Wie seht ihr diese Initiative?

Ja, also, wir haben jetzt mal eine erste Präsentation bekommen von dem, was da vorgesehen wird, und wir haben sehr stark das Gefühl, dass einfach auf die zwei, drei Fälle reagiert wird, die wir bisher gehabt haben, das war halt die Situation rund um Facebook und EDSA-Entscheidungen inzwischen gegen Irland. Aber eigentlich werden viele darunterliegende Probleme strukturell nicht angegangen. Also, wir brauchen zum Beispiel einfach klare Regeln, wann welches Verfahrensrecht anwendbar ist. Wenn ich jetzt zum Beispiel eine Beschwerde einbringe, dann kann ich das ja nur nach dem Verfahrensrecht von dem jeweiligen Land machen, wo ich gerade bin. Gleichzeitig wendet aber die federführende Behörde einfach ihr Verfahrensrecht an, auch auf die Beschwerde, die in irgendeinem anderen Land eingebracht wird. Und da gibt es sehr viele solche grundsätzlichen Fragen, wo man sagen muss, wenn man das einmal klarstellen würde und sagen, gut, hier endet die Jurisdiktion von der Concerned Authority, da fängt sie von der Lead Authority an. Mit den Elementen kann man schon recht gut dann viele von diesen Streitereien oder Problemen ausräumen.

Wir sehen jetzt eher, dass die Kommission probiert mit einer Art Beschwerdeformular, mit einer Kooperation sozusagen, die ein bisschen früher beginnt zwischen den Behörden, aus den aktuellen Problemen zu lernen. Also das wäre ja auch an sich sinnvoll, aber dass die strukturellen drunter liegenden Probleme, die einfach prozessrechtliche Grundsatzprobleme sind, damit nicht wirklich gelöst werden, ist meine Befürchtung.

Und damit wäre eigentlich eine große Chance vielleicht vertan. Und das Problem ist auch, dass irgendwie Verfahrensrecht halt nicht sexy ist. Also ist das politisch uninteressant, keiner macht dazu groß irgendwas. Aber es ist unterm Strich sozusagen das, was im Maschinenraum die Sache am Laufen hält oder halt nicht am Laufen hält. Und da ist deutlich mehr zu tun, als das, was die Kommission jetzt aktuell so anscheinend plant.

Es gab ja da eine public consultation[4] mit einem Dokument der Kommission und dazu hat noyb auch eine Stellungnahme eingereicht.

Ja, ich glaube, die längste und fetteste. Wir haben aus unserer Erfahrung wirklich geschaut, wo wir überall schon Probleme gehabt haben. Wir haben eine Problemliste von über 60 faktischen Problemen, die du wirklich am Boden der Tatsachen in Verfahren hast, aufgestellt. Und haben probiert aus diesen Problemen Konzepte herauszuarbeiten, mit welchem grundsätzlichen Konzept man jedes dieser Probleme lösen könnte. Also zum Beispiel mit einer klaren Festlegung, welches nationale Recht wann anzuwenden ist, könnte man schon recht viele Probleme klären. Wenn man dann einfach sagt, gut, der eine ist zuständig, dann ist es so und dann wissen wir es auch.

Oder dass man sagt, es gibt gewisse Minimumstandards, wo man sagt, zumindest muss jeder Akteneinsicht haben, zumindest muss jeder irgendwie gehört werden. Diese Dinge, das sind ja auch Sachen, die eigentlich unstrittig sind, muss man sagen. Und ich glaube,

mit diesen Grundsatzkonzepten würden wir sehr weit kommen, weil man halt wie immer mit einer sehr abstrakten Regelung viel erreichen kann, wenn sie gut geschrieben ist. Und aus dem heraus haben wir sogar eine Verordnung, wie man sie schreiben könnte, mal vorgelegt. Die ist jetzt nicht perfekt und die ist nicht final, aber bei der man zumindest eine Idee hätte, wie so eine Struktur ausschauen könnte, die einfach Sinn ergibt. Und die Idee davon war eben nicht das jetzt sehr „pro Datenschutz" zu machen oder sich in irgendeine Richtung zu bewegen, sondern wirklich sich zu überlegen, wie machen wir die Zivilverfahrensordnungen, die es gibt, also Small Claims Procedure, Europäisches Mahnverfahren, diese ganzen Sachen, die es ja schon gibt. Auch EGVVO, also da gibt es ja schon viele Modelle, wo man sieht, okay, das gibt es schon, das kennen die Juristen schon, das ist auch was, wo man den Leute nicht sozusagen prinzipiell neu erklären muss, was es ist, weil sie es schon aus anderen Rechtsbereichen kennen, und ich glaube mit so einem Zugang wird man wahrscheinlich deutlich weiterkommen.

Die Kommission hat über 70 Antworten[5] bekommen auf ihren Aufruf zum Call for Evidence, das heißt praktische Erfahrungsberichte, und sie möchte im zweiten Quartal 2023 einen neuen Bericht dazu veröffentlichen. Gibt es Aussagen von der Kommission zur Planung für eine gesetzgeberische Initiative?

Unser Informationsstand ist, dass sie es noch in dieser Legislaturperiode durchbringen wollen. Und das heißt aber auch, dass es in Wirklichkeit schon eine geschriebene Version gibt, während der Call for Evidence noch gelaufen ist. Und das macht jetzt, sagen wir mal, die Qualität vielleicht nicht unbedingt besser. Und das andere Problem, was wir dabei auch haben, ist, dass dieser Call for Evidence, um ehrlich zu sein, in der Qualität von den Inputs sehr überschaubar ist. Also, man merkt, dass es am Ende etwa 30 Industriepapers gibt. Sonst gibt es von uns was und von Access und EDRi kürzere Stellungnahmen. Aber es gibt sehr wenige, die in dem Bereich überhaupt Erfahrung haben. Und auch bei den Industriepapers sieht man, dass im Hintergrund sehr oft Facebook das instrumentalisiert hat, weil da ganz spezifisch zu ihrem Verfahren steht, was sie wollen.

Das ist dann von fünf, sechs Industrieverbänden, wo Meta dabei ist, wiederholt und wiederholt und wiederholt worden. Da sieht man auch, dass es von der Unternehmensseite wenig Substanz gibt, was die da wollen oder nicht wollen, weil die meisten Verfahren so stecken, dass eigentlich viele so ein Verfahren noch gar nicht durchgemacht haben. Auch von anderen NGOs, die in dem Bereich arbeiten, die wissen generell um die Probleme, aber sie haben selber auch nicht diese Hands-on-Erfahrung und man muss halt sagen, wir sind die einzigen, die aktuell über 800 Verfahren betreiben, die schon einen ganz guten Überblick haben, was alles schief geht und da glaube ich, ist auch das Problem sozusagen von dem Input zu dieser Regelung, dass die Kommission sich großteils auf das verlassen hat, was die Datenschutzbehörden wollen. Und da muss man aber sagen, dass jetzt sozusagen eine Behörde normalerweise nicht zu viel Interesse hat ein strenges Verfahrensrecht zu haben.

Es gibt ja einen Grund, warum wir auf europäischer Ebene auch für die Kommission kein Verfahrensrecht haben, wie wir es in Deutschland oder in Österreich kennen. Da hat man schon den Eindruck, dass man teilweise eher probiert die Verfahren loszuwerden. Oder zum Beispiel dieses französische Modell, wo man sagt, der Beschwerdeführer ist eigentlich gar nicht Partei, weil es ja nicht so ist, als ob es um seine Grundrechte gehen würde. Und da gibt es schon einen sehr starken Trend, dass man probiert sich nur mit den Unternehmen zu beschäftigen und nicht mehr mit den Betroffenen.

Und das ist teilweise verständlich, weil die Kommission selber sehr stark darauf schaut, was es bisher im Wettbewerbsrecht und im Kartellrecht gibt. Da hast du normalerweise eine abstrakte Figur, den Markt, den du schützt. Bei uns aber, beim Auskunftsersuchen, hast du einen ganz konkreten Hans Huber, der einfach seine Daten nicht bekommen hat oder die nicht gelöscht bekommen hat. Das ist kein öffentliches Interesse im Breiteren. Das ist ein Privatinteresse von einer Einzelperson. Da wird aber trotzdem jetzt versucht mehr oder weniger das französische Modell in Europa einzuführen, wo man sagt: „Naja, der ist so eine Art Hinweisgeber, aber sonst hat er eigentlich keine Rechte." Und das ist für mich halt schon extrem zynisch, wenn man sich denkt, wir haben ja da einen Grundrechtsschutz und wir haben da einen Betroffenen, der eine Meinung äußern will, er wird aber nicht gehört. Das macht einfach strukturell wenig Sinn.

Und es ist mir vollkommen bewusst, dass diese Beschwerden sehr mühsam sind und viele Beschwerdeführer auch sehr mühsam sind. Wir kriegen ja auch die E-Mails. Aber die Lösung kann nicht sein, dass wir einfach sagen „Die werden einfach gar nicht mehr gehört, im Bausch und Bogen." Und da merkt man aber schon, dass es da ein gewisses Interesse von den Datenschutzbehörden gibt, und die sagen uns das auch eigentlich durchaus direkt, dass sie halt jetzt probieren Beschwerden, die nicht genau Beschwerde nach Art. 77 DSGVO genannt werden, als reine informelle Anfragen zu behandeln. Damit kann man sein Beschwerdeaufkommen schon gut minimieren. Wir sehen das ganz extrem in Frankreich, in Schweden war es auch so, wo die gesagt haben, man hat überhaupt gar kein Beschwerderecht. Also man hat eigentlich nur so ein Petitionsrecht, dass man halt ein Recht hat die darauf aufmerksam zu machen, dass was ist. Aber man hat dann überhaupt kein Recht, dass die das irgendwie behandeln oder weiter was tun damit. Da haben wir in Schweden als noyb gegen die schwedische Behörde vor allen Gerichten gewonnen. Das ist jetzt in der letzten Instanz, aber bisher haben uns alle Gerichte Recht gegeben, dass die das schon bearbeiten müssen.

Aber da sieht man, dass die Behörden wirklich probieren diese Beschwerden loszuwerden. Und um ein bisschen raus zu zoomen, ich glaube wir haben halt ein Generalpräventionsproblem. Also natürlich, wenn auf fast jeder Webseite irgendwo Datenschutzverletzungen zu sehen sind, dann können viele Leute sich beschweren und werden sich auch viele Leute beschweren. Wenn es dann keine Durchsetzung gibt, wird dieser

Status so bleiben. Und ich glaube, wir müssen irgendwann einmal wirklich mit der Durchsetzung massiv reinfahren, in der Hoffnung, dass Unternehmen sich dann selbstständig schon dranhalten und damit auch das Beschwerdeaufkommen runtergeht.

Also ich habe bei uns permanent Datenschutzbeauftragte, die mich dann ansprechen und sagen „Danke, dass es zumindest Euch gibt, weil, auch wenn nichts rauskommt, allein dass es sozusagen Presseberichterstattung gibt und die Namen von den Unternehmen dann irgendwo öffentlich sind, das wirkt dann, dass dann doch jemand mal was tut, also bei mir im Unternehmen jeweils dann.“ Und da gibt es wirklich Leute, die sagen, wir als NGO seien der größere Faktor, dass sie ihren Chef überzeugen sich an die DSGVO zu halten, als die Aufsichtsbehörde. Und das kann halt nicht sein, dass wir als Verein da irgendwie relevanter sind, oder?

Gelten diese Beobachtungen eigentlich nur für grenzüberschreitende Verarbeitung oder ist es auch bei einfachen Fällen, die direkt in einem Mitgliedsstaat entschieden werden können, eine ähnliche Problematik, wie wir das bei diesen OSS-Geschichten haben?

Das ist sehr ähnlich. Wir haben auch national jetzt nicht wirklich große Tätigkeiten. Ich glaube, es ist ein bisschen verschieden pro Nation. Also wir sehen zum Beispiel, dass die spanische Behörde im Schnitt sechs, sieben Entscheidungen am Tag raushaut. Also da passiert schon was. Wir sehen zum Beispiel, dass die französische Behörde mit diesen Ex-offizio-Verfahren sehr stark ist. Auch muss man sagen, dass sie ihre Arbeit medial sehr gut verkauft. Also, es gibt schon da und dort ein bisschen mehr Aktivität, oder auch die Italiener haben in letzter Zeit ein bisschen mehr diese großen Headline-Geschichten gemacht. Nur fehlt es dann oft in der Breite. In Spanien zum Beispiel wäre vielleicht die Breite da, aber zum Beispiel bei der CNIL ist es so, dass die sagen, sie machen was zur Cookie-Problematik: 20 Verfahren. Bei einem Land wie Frankreich nur 20 Verfahren zu machen ist halt süß. Wenn du denkst, wir betreiben derzeit über 600 Verfahren zu Cookie Banners als eine deutlich kleinere Organisation, dann fehlt es da einfach sehr oft auch an der technischen Ausstattung. Wir machen das ja zum Beispiel mit einfachen Systemen, die das automatisch erkennen und die Beschwerden automatisch bauen und so weiter. Es ist noch immer viel Handarbeit, aber es ist sehr, sehr viel automatisiert. Ich glaube, da fehlt auch oft die Kreativität oder die Überlegung, wie man so etwas macht. Ich glaube, wir bräuchten sehr viele Beamte, die aus anderen Bereichen mit Erfahrung zur Rechtsdurchsetzung kommen, z.B. in der Durchsetzung von Steuerschulden.

Da ist es ja auch so, dass die Steuerbehörden durchaus kreativ sind und durchaus da einfach beim Unternehmen mal rein spazieren und sagen: „So, jetzt wollen wir mal haben, was ihr da in den Akten habt.“ Das ist eine ganz andere Herangehensweise, als wir sie im Datenschutz kennen. Und ich glaube, diese Kultur wäre teilweise wichtig. Wir haben halt diese Cookie-Banner-Systematik, wo wir praktisch Webseiten scannen auf Rechtsverstöße. Ich sehe das so ähnlich wie so eine Geschwindigkeitskamera. Die macht automatisch ein Bild, rechnet automatisch das Kennzeichen raus, sucht dann im Kennzeichenregister, wer der Halter ist und schickt dem Halter die Rechnung zu oder halt den Strafzettel. Und das schaut sich zumindest in Österreich kein Mensch an. Also das passiert alles automatisch.

Bis irgendeiner sagt, da gibt es einen Fehler und wenn sich jemand beschwert, dann wird menschlich überprüft. Aber zu 99 Prozent zahlen die Leute halt einfach ihre Strafe, weil sie wissen, dass es einfach eine Geschwindigkeitsübertretung war. Und dann hat es sich auch. Das Spannende ist, dass wir diese digitalen Massenverletzungen eigentlich mit absolut analogen Mitteln gerade bekämpfen. Und wo endlose Schriftsätze geschrieben werden und eigentlich selten wirklich technisch analysiert wird, was da wirklich passiert, sondern das sagt halt ein Anwalt „Nein, das machen wir gar nicht und das speichern wir gar nicht.“ und der andere sagt „Doch, wir glauben schon, dass ihr das speichert.“ und keiner geht hin und überprüft es einfach. Und damit hast du diese endlosen, wirklich sehr sinnlosen Ping-Pong-Geschichten, wo in jedem anderen Rechtsbereich einfach der Sachverhalt vom Gericht geprüft wird. Bei einer Bauverhandlung z.B. gibt es einen Lokalaugenschein, dann wird geschaut und gemessen und sonst was, wie hoch das Haus beispielsweise sein darf.

Und dann ist es so. Dann hat man halt zwei Stunden mündliche Verhandlungen und dann wissen es auch alle. Und da gibt es schon Ansätze. Also zum Beispiel in Belgien gibt es mündliche Verhandlungen, wo auch mir zumindest die Beamten dort gesagt haben, dass das durchaus effektiv ist, weil man dann einfach in zwei Stunden alle an einem Tisch hat und dann wird ausgeredet und dann ist es das. Aber das ist alles sehr, sehr in den Kinderschuhen und ich glaube, da fehlt wirklich sehr viel Management von Verfahren und Verfahrensoptimierung.

Es gab ja auch interessante Initiativen von finanzkräftigen Gruppen, die Zivilverfahren zur DSGVO in Großbritannien, als es noch Mitglied der EU war, und auch in den Niederlanden gestartet haben. Jetzt hört man länger nichts mehr. Läuft diese Schiene noch oder ist das angesichts der Probleme mit den Zivilgerichten eingeschlafen?

Ich glaube, dass da zum Teil eine gewisse Frustration da ist. Diese Durchsetzungsschiene funktioniert dann, wenn das Ganze effektiv ist und auch was bringt. Und wir sehen, dass die Richter wirklich probieren diese Fälle loszuwerden. Zu vielen Faktoren gibt es bisher keine EuGH-Rechtsprechung und das Risiko ein Verfahren zu machen, wo die Kosten eine Million Euro sind – also, die Verfahrenskosten von so großen Verfahren sind ja wirklich riesig, wenn du keine wirklich stabile Rechtslage hast, also gerade zum Schadenersatz in den Bereichen – dann macht das keiner.

Ich glaube, jetzt warten auch alle ein bisschen, was der EuGH so sagt zu dem Thema. Dann kann man planen, dann kann man sagen, gut in dem Fall haben wir es und in dem Fall haben wir es nicht. Wo das jetzt – glaube ich – wieder aufflackern kann, ist, dass wir ab Sommer die

europäische Sammelklage haben, also diese Collective Redress Directive, und da gibt es die Möglichkeit eben Schadenersatz auch kollektiv durchzusetzen und also vor allem Datenschutz kollektiv durchzusetzen, so wollte ich sagen. Und das wäre schon eine Option, wo wir das vielleicht wieder sehen. Das hängt aber eben sehr stark mit der Frage von Schadenersatz zusammen, weil, wenn ich jetzt eine Klage habe, die eine Million Euro in Kosten hat, gegen irgendeinen von diesen Großkonzernen in teureren Ländern, das schnell erreicht ist.

Wenn das Einzige, was ich da einklage, eine Unterlassung ist, dann ist das eine Geldverbrennung. Weil ich dann eine Million Euro Kosten zahle, und vielleicht kriege ich 100.000 Euro zurück. Aber wer zahlt 900.000 Euro dafür, dass da irgendeine Unterlassung durchgesetzt wird?

Sobald ich hingegen einen Schadenersatzanspruch habe – und ich glaube, Schadenersatz sollte halt auch im Datenschutzbereich nicht irgendwie exorbitant oder crazy sein – aber sobald eine gewisse Summe dasteht, kann ich das Ganze schon finanzieren, weil ich dann das Ganze sozusagen mit Prozesskostenfinanzierung machen kann und da gibt es eine Möglichkeit, dass erstens die Leute, die Betroffenen, auch was davon bekommen, dass zweitens die Unternehmen auch was spüren davon, im Gegensatz zur reinen Unterlassung für 10.000 Leute, wo ich einfach diese 10.000 Accounts lösche und ansonsten weitermache wie bisher. Wenn es einen Schadensersatz gibt, kann man halt sagen, gut von dem, was da gewonnen ist, gehen 5% oder 10% an die Finanzierung der Klageführung. Und bei der Collective Redress Directive ist es eh so, dass die Vereine, die das organisieren, und das werden zum Beispiel jetzt wir, selber überhaupt nichts daran verdienen dürfen.

Das ist sehr anders bei der amerikanischen Sammelklage. Aber natürlich wird es gerade am Anfang sehr schwierig sein, weil die meisten beklagten Unternehmen sagen werden, dass das amerikanische Zustände sind und alles ist ganz crazy und ganz schlimm. Viele Richter werden das wahrscheinlich auch intuitiv erst einmal so sehen. Und das ist ein großer Faktor, der bei uns reinspielt, das ist einfach die Emotion. Also, du kannst die beste Argumentation haben und den besten Fall haben. Wir sehen das dann so vor Gericht, dass einfach viele sagen, das ist ja dieses blöde Gesetz mit den Cookie-Banners, das finde ich blöd, da mache ich nichts. Also das ist sehr überspitzt gesagt, aber unterm Strich ist es das. Und ich habe selber einen Fall gehabt, wo mir über einen anderen Kanal dann mitgeteilt worden ist, dass die Entscheidungsträger einfach die DSGVO blöd finden und deswegen dagegen entschieden haben.

Ja, vielen Dank. Man kann natürlich jetzt im Augenblick nicht ein Interview mit Max Schrems führen ohne ein mögliches EuGH-Urteil zum nächsten Versuch der Kommission, die Angemessenheit eines US-amerikanischen Verfahrens für die Verarbeitung von Daten zu erlangen, zu erwähnen. Da hat die Biden-Regierung jetzt eine Konstruktion vorgelegt, die sicherlich besser ist als alles, was es je gab. Und die Kommission ist ja gerade dabei ihre Angemessenheitsentscheidung vorzubereiten. Und es ist wohl sicher, dass es kein Schrems-III-Urteil des EuGH geben wird, weil der EuGH nicht mehr die Namen von Einzelpersonen in der Bezeichnung von seinen Verfahren verwendet.

Ich glaube die Allgemeinheit würde es trotzdem so nennen. Ja, also wir wissen ja faktisch, dass es politisch beschlossen worden ist, und wir wissen auch, dass das jetzt so kommen wird. Also, da braucht man nicht so tun, als ob da jetzt noch wirklich groß irgendwas herum entschieden wird. Das ist einfach politisch gewollt und das wird so gemacht. Insofern wissen wir schon ganz gut, was da ist. Wir kennen jetzt schon große, große Lücken in dieser Executive Order und es ist richtig, es ist ein bisschen besser in vielen Bereichen. Es ist in einigen Bereichen auch schlechter. Also, wenn man diese neue Executive Order mit der PPD 28 vergleicht, dann gibt es Teilbereiche, wo jetzt auch mehr Überwachung zugelassen wird. Also, zum Beispiel soll jetzt Massenüberwachung zulässig sein im Kampf gegen Pandemien oder gegen den Klimawandel. Das ist vorher nicht dagestanden. Also, es ist nicht nur besser geworden. Es gibt auch Bereiche, wo man fragen kann, ob das nicht eine Ausweitung ist. Ich glaube, es ist so ein bisschen Silicon Valley-Sprechweise: „let's fail better next time". Also im Sinne von, wir machen schon ein bisschen besser, aber wir kommen noch immer nicht über die Hürde drüber.

Ich sage immer, es ist nett, wenn man einen Gartenzaun baut und das erste Mal war er 5 cm und jetzt ist er 5,5 cm und das nächste Mal ist er 7 cm. Aber das ist trotzdem kein Gartenzaun, der irgendjemanden abhält. Und ich glaube, das ist so – sehr bildlich gesprochen – das Spiel, das wir da gerade spielen.

Und es ist auch, muss ich sagen, für die Kommission schwierig, wenn die auf der einen Seite sagt, sie sind der Hüter des Rechtsstaats und irgendwelche bösen, bösen ungarischen und polnischen Despoten halten sich ja nicht an EuGH-Urteile. Und dann verabschiedest du halt selber das gleiche Ding wieder und wieder. Und ja, du machst schon ein bisschen was anders, aber es ist jetzt keine grundsätzliche Änderung. Also gerade von Safe Harbor auf Privacy Shield, das war im Prinzip der gleiche Text. Dann ist es, finde ich, auch eine Glaubwürdigkeitsfrage oder auch ein politisch größeres Problem.

Oder wenn man sagt „Gut, dieses Gericht, was jetzt in den USA da besteht, das ist ja absolut compliant mit Artikel 47 der Grundrechte-Charta und ein ordentlicher Gerichtsprozess" – wo du ja nicht mal als Partei weißt, was entschieden worden ist oder sonst was. Und gleichzeitig sagen wir aber, in Ungarn und Polen haben wir Riesenprobleme mit der Rechtsstaatlichkeit nach Artikel 47. Das kriegst du ja nicht unter einen Hut. Und das wird auch für den EuGH schwierig sein. Selbst wenn der EuGH fünf neue Richter dort hat, die das alles anders sehen, wird es sehr schwierig sein zu sagen „Naja, ein Nichtgericht in den USA ist compliant mit Artikel 47, aber Polen und Ungarn sind es absolut nicht."

Zum Schluss noch ein paar Worte zu „neu": noyb hat ja auch insgesamt 800 Verfahren angestrengt (siehe gdprhub.eu) wo Entscheidungen und Urteile zu den verschiedenen Artikeln der DSGVO gesucht werden können.

Wobei sonst könnten Mitglieder der DVD von noyb noch Nutzen ziehen oder vielleicht auch selbst beitragen?

Ja, ich glaube, die Informationsseite, die wir hauptsächlich haben, ist gdprhub.eu[6], die für Professionisten interessant ist, wo wir einfach die Urteile zusammenfassen. Dann hat man zumindest eine Idee, was global oder europäisch entschieden wird. Der Newsletter dazu, der das zusammenfasst, ist GDPR Today. Wo wir jetzt mehr machen, ist, dass wir auch in Richtung Kommentar online gehen und probieren das Know-how weiter zu stärken. Weil wir in vielen Bereichen – also der klassische Leser von euch ist vielleicht schon sehr tief im Thema drinnen – sehr viele Entscheidungsträger in irgendwelchen Unternehmen haben, die eigentlich nicht wirklich wissen, was in der DSGVO drinnen steht. Die haben halt für oft viel Geld irgendeine schnelle Zertifizierung gemacht, aber man merkt dann sehr schnell, dass eigentlich das Verständnis nicht tief da ist. Und ich glaube, da gibt es noch sehr viel Raum, dass man was tut. Das ist das eine. Und andererseits ist bei uns generell immer die Möglichkeit, dass man sich als Mitglied engagiert, hauptsächlich finanziell.

Aber auch was bei uns recht häufig ist oder gewollt ist, ist, dass man z.B. Tippgeber ist, auf etwas hinweist, wo ein Problem ist, was wir uns anschauen können. Da ist es auch für uns immer gut, wenn man einen qualifizierten Input hat, weil es ja oft strukturelle Probleme gibt, zum Beispiel bei Auftragsverarbeitern, die ganz viele Verantwortliche bedienen. Also wenn einfach oft hunderte Verantwortliche das gleiche Problem haben, aber keiner einzeln was tut, dann ist es für uns auch teilweise interessant, dass wir dann zum Beispiel gegen den Dienstleister vorgehen, wenn wir die Informationen erst mal überhaupt dazu haben. Also gerade solche Sachen sind eigentlich immer interessant.

Vielen Dank für das Gespräch.

Anmerkung: Nach dem Gespräch entschied der EuGH in mehreren Fällen: In dem im Interview erwähnten Fall zur Einschätzung der politischen Haltung von Kunden der österreichischen Post entschied der EuGH[7], dass zwar ein Verstoß gegen die DSGVO nicht automatisch einen Schadensersatz begründet, dass es aber andererseits keine Erheblichkeitsschwelle oder Bagatellgrenze gibt.

In einem anderen Fall[8] wurde entschieden, dass der Auskunftsanspruch der Betroffenen die vollständige Kopie der Unterlagen umfasst, die der Verantwortliche hält.

1 https://noyb.eu/de.

2 Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_de.

3 Verbindliche Entscheidungen des EDSA in den von der irischen DSA eingereichten Streitigkeiten zu Facebook, WhatsApp und Instagram vom 5. Dezember 2022 u.a.; https://edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_de.

4 Datenschutz-Grundverordnung – Verfahrensvorschriften für die Durchsetzung; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_de.

5 73 Rückmeldungen; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation/feedback_de?p_id=31874182.

6 https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub.

7 Urteil des Gerichtshofs in der Rechtssache C-300/21 – Österreichische Post (Immaterieller Schaden im Zusammenhang mit der Verarbeitung personenbezogener Daten); https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-05/cp230072de.pdf.

8 Urteil des Gerichtshofs in der Rechtssache C-487/21 – Österreichische Datenschutzbehörde und CRIF; https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-05/cp230071de.pdf.


Max Schrems bei einer DVD-Veranstaltung 2012 im Europa-Parlament in Brüssel

Bild: Frans Valenta

Axel Freiherr von dem Bussche, Alexander Schmalenberger

Ausgewählte Rechtsetzungsinitiativen der Europäischen Union im Zeitalter der digitalen Revolution: Chancen, Herausforderungen und offene Fragen des Datenschutzes

Einleitung

Die digitale Revolution hat tiefgreifende Veränderungen in unserer Gesellschaft bewirkt und wird auch in Zukunft eine bedeutende Rolle spielen. Die Europäische Union (EU) hat verschiedene legislative und nicht-legislative Initiativen und Instrumente entwickelt, um angemessen auf diese digitale Revolution zu reagieren.[1] Diese Maßnahmen betreffen die öffentliche Verwaltung, die Wirtschaft und die Bürger und zielen darauf ab Kompetenzen aufzubauen und einen Rechtsrahmen für eine gesunde digitale Entwicklung zu schaffen. Dieser Fachbeitrag konzentriert sich auf die aus Sicht der Autoren praktisch relevantesten Fragen und legt den Schwerpunkt auf die Regelungen zur Datenverarbeitung und deren Auswirkungen auf das Recht auf informationelle Selbstbestimmung. Dazu sollen im ersten Teil die wichtigsten Gesetze und ihre Beziehungen zum Datenschutz betrachtet werden. Allen Regelungen ist gemein, dass die Datenschutz-Grundverordnung (DSGVO) „unberührt" bleiben soll – ob das stimmt, wird im zweiten Teil behandelt. Diesem folgt ein Fazit.

Die Gesetze

Im folgenden Abschnitt analysieren wir verschiedene rechtliche Regelungen zur Datenverwendung. Dazu gehören der Digital Services Act, der Digital Markets Act, der Data Act, das Data Governance-Gesetz, der European Health Data Space und der Artificial Intelligence Act. Diese Gesetze begrenzen einerseits die Datennutzung großer Unternehmen. Andererseits fördern sie die Datenfreigabe, um Innovation und Wirtschaftswachstum zu stimulieren. Dabei gilt es ein Gleichgewicht zwischen Datenschutz und Datenökonomie zu finden.

Der Digital Services Act (DSA) modernisiert die Regelungen für Online-Plattformen und Intermediäre, einschließlich derer, die außerhalb der EU sitzen, aber dort tätig sind. Er betont die Pflichten in Bezug auf Transparenz, Rechenschaft, Zusammenarbeit mit Behörden und Schutz vor illegalen Inhalten. Er schreibt fest, dass Plattformen zur Verantwortung gezogen werden können, wenn sie personenbezogene Daten verarbeiten und dass Nutzer das Recht auf Beschwerdemechanismen und auf Zugang zu Informationen haben. Der DSA verstärkt die DSGVO und setzt Grenzen bei der Datenverwertung: Art. 26 und 28 DSA setzen der Nutzung von personenbezogenen Daten bei der Werbung engere Grenzen, als dies unter der DSGVO allein bisher der Fall gewesen ist. Große Plattformen wiederum müssen datensparsame Empfehlungssysteme anbieten (Art. 38 DSA).

Der Digital Markets Act (DMA) zielt darauf ab faire Bedingungen in digitalen Märkten zu schaffen und missbräuchliche Praktiken von dominierenden Plattformen, den sogenannten „Gatekeepern", zu verhindern. Der DMA verbietet Gatekeepern personenbezogene Daten ohne Zustimmung der Nutzer nach Art. 7 DSGVO für Werbezwecke zu verarbeiten oder zwischen verschiedenen Plattformdiensten zu teilen. Er gewährt den Nutzern das Recht auf Datenübertragbarkeit und Schutz vor unfairen Bedingungen.

Das Data Governance Act (DGA) regelt die Verfügbarkeit, Nutzung und Weitergabe von Daten in der EU, insbesondere von solchen, die nicht unter die DSGVO fallen. Es legt Standards für Qualität, Sicherheit und Vertrauen bei der Datenverarbeitung fest. Nutzer haben das Recht auf Zugang zu hochwertigen Daten und können an Initiativen zur Datenfreigabe teilnehmen, wobei ihre Interessen geschützt bleiben.

Der vorgeschlagene Data Act ist eine Erweiterung des DGA und zielt darauf ab die Verfügbarkeit und Weitergabe von Daten in der EU zu verbessern, vor allem von Daten, die aus industriellen und kommerziellen Aktivitäten stammen oder für das Gemeinwohl relevant sind. Er legt Regeln für den Zugang und die Nutzung von ausgetauschten Daten fest und gewährt den Nutzern das Recht auf Teilnahme an Datenkooperationen. Es ist aber absehbar, dass auf Grundlage des Data Act – insbesondere im Kontext von IoT – auch personenbezogene Daten getauscht werden könnten.

Der Data Act soll nach seiner Konzeption allerdings nur dann gelten, wenn es keine spezielleren Regelungen gibt. Etwa solche, die Datenräume für bestimmte Anwendungsfälle regeln. Ein Beispiel ist der European Health Data Space (EHDS), der derzeit im Gesetzgebungsverfahren behandelt wird. Der EHDS soll einen gemeinsamen Raum für Gesundheitsdaten in Europa schaffen, um die Zusammenarbeit und Innovation im Gesundheitswesen zu fördern. Er legt Regeln für die Verarbeitung, den Schutz und die Nutzung von Gesundheitsdaten fest und gewährt den Nutzern das Recht auf Zugang zu Gesundheitsdaten.

Der Artificial Intelligence Act (AIA) soll einen einheitlichen Rechtsrahmen für künstliche Intelligenz in der EU schaffen. Tatsächlich aber enthält der Vorschlag z.B. in Art. 10 Abs. 5 AIA einen Erlaubnistatbestand zur Verarbeitung sensibler Daten im Sinn des Art. 9 DSGVO, um Verzerrungen (Bias) in Hochrisikosystemen zu erkennen und zu beheben. Im Umkehrschluss könnte die Verarbeitung dieser Daten in allen anderen Fällen damit verboten sein. Aber müssten sie nicht vorher gespeichert werden? Für Reallabore (Sandboxes, Art. 54 AIA) wiederum wird die Verarbeitung von Daten erlaubt. Damit liegt

ein Erlaubnistatbestand vor. Vermutlich wird das Europäische Parlament im Rahmen des Trilogs vorschlagen, dass für Hochrisiko-Anwendungen dann eine Zusammenfassung der Datenschutz-Folgenabschätzung veröffentlicht werden muss.[2]

Das ungeklärte Verhältnis zur DSGVO

Die hier vorgeschlagenen Rechtsakte enthalten Klauseln, die die Anwendbarkeit der DSGVO auf die Verarbeitung personenbezogener Daten im Zusammenhang mit den jeweiligen Regelungsbereichen bestätigen – die DSGVO bleibt „unberührt" – jedoch bei näherer Betrachtung einschränken oder modifizieren. Diese Klauseln sind in Bezug auf Klarheit, Kohärenz und Konsistenz unterschiedlich formuliert. Dies kann zu Rechtsunsicherheit, Inkohärenz und möglichen Konflikten zwischen den verschiedenen Rechtsakten führen.

Der DSA enthält eine Unberührtheitsklausel (Art. 2 Abs. 4 DSA), die besagt, dass die Verordnung die Anwendbarkeit der Rechtsvorschriften der Union über den Schutz personenbezogener Daten, insbesondere der DSGVO und der ePrivacy-Richtlinie, nicht berührt. Damit nicht vereinbar ist jedoch, dass der DSA Online-Plattformen und Hostingdiensteanbietern bestimmte Pflichten auferlegt, die die Verarbeitung personenbezogener Daten von Nutzern und Dritten erfordern ohne eine klare Rechtsgrundlage oder Garantien dafür zu bieten, und dass der DSA mit dem Grundsatz der Datenminimierung und dem Recht auf Löschung gemäß der DSGVO kollidieren könnte. So verlangt Art 23 DSA, dass Plattformbetreiber Maßnahmen gegen die missbräuchliche Verwendung ihrer Dienste oder der Melde- und Abhilfeverfahren vorsehen – dazu wird es aber erforderlich sein die notwendigen personenbezogenen Daten zu erheben und zu speichern.

Der DMA enthält ebenso eine Unberührtheitsklausel (Art. 5 Abs. 2 DMA), die besagt, dass die Verordnung unbeschadet der Bestimmungen gilt, die sich aus anderen Rechtsakten der Union ergeben, insbesondere der DSGVO. Nichtsdestotrotz sieht der DMA z. B. in Art. 5 Abs. 2 bestimmte Verhaltenspflichten für Gatekeeper vor, die die Einwilligung der Nutzer in die Verarbeitung personenbezogener Daten voraussetzen, ohne andere mögliche Rechtsgrundlagen zu berücksichtigen. Unklar ist, ob diese damit ausgeschlossen sind. Wenig hilfreich ist auch, dass der Art. 7 Abs. 8 DMA den Begriff „unbedingt erforderlich" verwendet, der in der DSGVO nicht definiert ist.

Der DGA enthält in Art. 1 Abs. 3 DGA eine Geltungsklausel, eine Vorrangklausel, eine Rechtsgrundlageklausel und eine Unberührtheitsklausel, die alle betonen, dass die DSGVO für alle personenbezogenen Daten gilt, die im Rahmen des DGA verarbeitet werden, und dass die DSGVO im Falle eines Konflikts zwischen dem DGA und dem Datenschutzrecht Vorrang hat. Vor diesem Hintergrund ist kritikwürdig, dass der DGA eine allgemeine Meldepflicht für die Verarbeitung personenbezogener Daten durch Datenlieferanten, Datenmittler und Datenverarbeiter einführt, was im Widerspruch zur DSGVO steht. Dort gibt es keine Meldepflichten. Darüber hinaus stellt sich die Frage der Vereinbarkeit mit dem Zweckbindungsgrundsatz, den Rechtsgrundlagen und der Weiterverarbeitung der DSGVO, insbesondere im Hinblick auf die Bereitstellung von Daten für gemeinnützige Zwecke und die Weitergabe von Daten an Dritte.

Der AIA sollte nach dem Willen der Kommission in der Begründung des Entwurfs die DSGVO unberührt lassen und enthält voraussichtlich eine Ergänzungsklausel, die besagt, dass die Verordnung die DSGVO unberührt lässt und durch harmonisierte Vorschriften für bestimmte Hochrisiko-KI-Systeme und biometrische Fernidentifizierungssysteme ergänzt wird. Damit würde der AIA ein datenschutzrechtliches Verbot für die Verarbeitung sensibler Daten durch Anbieter von Hochrisiko-KI-Systemen schaffen, das nur unter bestimmten Voraussetzungen aufgehoben werden kann. Darüber hinaus könnte der AIA eine Erlaubnisnorm nach Art. 6 Abs. 4 DSGVO darstellen, die die Verarbeitung personenbezogener Daten zu anderen Zwecken als denen, zu denen sie erhoben wurden, erlaubt; nach dem voraussichtlichen Willen des Europäischen Parlaments insbesondere auch für den Test neuer Anwendungen.[3] Diese Regelungen werfen Fragen nach der Vereinbarkeit mit den Grundsätzen der Zweckbindung und der Rechtsgrundlage der DSGVO auf.

Der Data Act enthält in der Fassung der Verhandlungsmandate[4] eine Unberührtheitsklausel (Art. 1 Abs. 3 Data Act), die besagt, dass die Verordnung die Rechtsvorschriften der Union über den Schutz personenbezogener Daten, den Schutz der Privatsphäre, die Vertraulichkeit der Kommunikation und die Integrität der Endgeräte unberührt lässt. Dies berücksichtigt aber nicht, dass der DA bestimmte Rechte und Pflichten für Dateninhaber, Datennutzer und Datenmittler vorsieht, die die Verarbeitung personenbezogener Daten zum Zwecke der Datenportabilität, der Datenübertragbarkeit, des Datenzugangs und der Datennutzung beinhalten, ohne dass eine ausreichende Abstimmung mit den entsprechenden Bestimmungen der DSGVO gewährleistet ist.

Der geplante EHDS[5] enthält in Art. 1 Abs. 3, 4 EHDS eine Unberührtheitsklausel, die besagt, dass die Verordnung andere Rechtsakte der Union über den Zugang zu elektronischen Gesundheitsdaten, deren Austausch oder Weiterverwendung sowie die Anforderungen an die Verarbeitung elektronischer Gesundheitsdaten, insbesondere die Datenschutz-Grundverordnung, unberührt lässt. Auch hier wiederholt sich der Befund, dass der EHDS bestimmte Mechanismen und Verfahren für die Verarbeitung von Gesundheitsdaten für die Zwecke der grenzüberschreitenden Gesundheitsversorgung, der öffentlichen Gesundheit, der Forschung und der Innovation vorsieht ohne eine klare Abgrenzung zu bestehenden oder geplanten Rechtsrahmen für die Verarbeitung solcher Daten vorzunehmen.

Fazit

Die EU-Digitalpolitik strebt einen ausgewogenen Rechtsrahmen an, der Datenschutz sicherstellt und Innovation fördert. Ihre Stärken liegen in der Harmonisierung von Rechtsrahmen und der Schaffung fairer Bedingungen für digitale Märkte. Datenschutz und Privatsphäre sind Kernpunkte, unterstrichen durch die DSGVO. Herausforderungen sind die Komplexität der Initiativen und die Notwendigkeit neue Technologien

wie KI zu regulieren. Internationale Zusammenarbeit ist unerlässlich, um den globalen digitalen Raum zu regeln.

Zukünftige Schwerpunkte sollten die Stärkung der Zusammenarbeit zwischen den Mitgliedsstaaten und die Sensibilisierung der Bürger für ihre digitalen Rechte sein. Es ist wichtig Transparenz und Rechenschaftspflicht von Unternehmen zu fördern und die Auswirkungen der digitalen Revolution auf die Demokratie zu erforschen. Trotz bereits vorgeschlagener Rechtsakte bleibt die Anpassung an die digitale Gesellschaft eine Herausforderung.

Eine kontinuierliche Überprüfung, Anpassung und Koordination der Rechtsvorschriften sind notwendig, um die Wirksamkeit der EU-Digitalpolitik zu gewährleisten. Dabei sollte auf Verhältnismäßigkeit, Effizienz und Transparenz geachtet werden. Die EU sollte eine aktive Rolle in der internationalen Zusammenarbeit spielen und Verstöße gegen digitale Rechtsvorschriften wirksam ahnden. Die Förderung von Forschung und Innovation in digitalen Technologien ist ebenfalls von großer Bedeutung.

Bildungs- und Sensibilisierungsmaßnahmen können dazu beitragen, dass Bürger ihre digitalen Rechte besser verstehen und schützen können. Eine enge Zusammenarbeit zwischen Regierungen, Unternehmen, Zivilgesellschaft, Forschungseinrichtungen und Verbraucherschutzorganisationen ist notwendig, um einen ausgewogenen Rechtsrahmen zu schaffen. Durchsetzung von digitalen Rechtsvorschriften ist entscheidend für das Vertrauen der Bürger.

Die EU sollte die Förderung von Forschung und Innovation im Bereich der digitalen Technologien vorantreiben und dabei ethische Standards fördern. Eine globale Führungsrolle der EU bei der Festlegung internationaler Standards für Datenschutz und digitale Rechte ist von entscheidender Bedeutung. Die Schaffung eines umfassenden und ausgewogenen Rechtsrahmens für die digitale Revolution bleibt eine komplexe und fortlaufende Aufgabe. Es ist wichtig, dass die Schaffung eines wirksamen Rechtsrahmens von einer breiten Beteiligung aller relevanten Akteure begleitet wird.

1 Vgl. die Studie Identification and assessment of existing and draft EU legislation in the digital field von Codogne, Liva, Rodriguez de las Heras Ballel, EPRS 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703345/IPOL_STU(2022)703345_EN.pdf, die Studie ist freilich Stand Januar 2022.

2 Vgl. DRAFT Compromise Amendments on the Draft Report Proposal for a regulation of the European Parliament and of the Council on harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9 0146/2021 – 2021/0106(COD)), https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf.

3 Ebd.

4 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Version for Trilogue on 29 March, 2023, https://www.europarl.europa.eu/RegData/publications/trilogue/2022/0047/NEGO_CT(2022)0047(2023-03-28)_XL.pdf.

5 Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197.

Thilo Weichert

Überlegungen zu einer datenschutzkonformen europäischen Forschungsregulierung

I Vorbemerkungen

Konsequent verfolgen die EU-Institutionen die Gesetzgebungsakte zur Umsetzung ihrer Digitalstrategie.[1] Selbst Insidern schwirrt der Kopf angesichts der Vorschläge zu digitalen Märkten, Diensten, Datenräumen, zu sog. künstlicher Intelligenz, Datentreuhändern und Sekundärnutzungen. Das Ziel ist weltweit bei der Digitalisierung an die Spitze zu gelangen. Angesichts des Umstands, dass die europäische Digitalwirtschaft in vieler Hinsicht von den USA und China abgehängt ist, drängt sich ein Spruch Walter Ulbrichts aus dem Jahr 1957 auf, der mit der Wirtschaft der DDR die des Westens „überholen ohne einzuholen" wollte. Ulbricht scheiterte damit. Ob die EU mit ihrer Offensive erfolgreich sein wird, hängt von Vielem ab: Einige EU-Mitgliedsstaaten können mit ihrer Digital-Infrastruktur und -Wirtschaft mit den IT-Zentren in den USA und China mithalten. Deutschland war bisher Mittelmaß. Die rot-grün-gelbe Bundesregierung hat trotz vollmundiger Ankündigungen[2] bisher wenig Vorzeigbares auf den Weg gebracht. Die Abhängigkeit Europas von US-amerikanischer Software und chinesischer Hardware ist gravierend; eine wirkliche Trendwende ist noch nicht erkennbar.

Doch auch die globalen Spitzenreiter schwächeln: US-IT-Unternehmen haben jüngst massenhaft Mitarbeitende entlassen, als wäre der IT-Hype am Ende. Zugleich wird aber mit ChatGPT die nächste IT-Sau durchs globale digitale Dorf gejagt, ohne Rücksicht auf die gesellschaftlichen Konsequenzen. Elon Musk führt mit halsbrecherischer Genialität bei Twitter vor, wie ein Privatkapitalist unsere demokratischen, freiheitlichen und rechtsstaatlichen Werte in Frage zu stellen in der Lage ist. Die chinesischen IT-Unternehmen

haben ihren Knowhow-Diebstahl vom Westen bei gleichzeitiger Abschottung soweit perfektioniert, dass sie technologisch zu den Unternehmen des Silicon Valley aufgeschlossen haben. Der von der Kommunistischen Partei staatlich gelenkte Digital-Kapitalismus Chinas könnte aber auch einen Dämpfer bekommen, wenn der Westen die Risiken erkennt, die mit seiner China-Kooperation für Demokratie und Freiheit wie auch für die eigene Wirtschaft verbunden sind, und daraus Konsequenzen zieht.

Es ist daher nicht abwegig, wenn Europa in Sachen demokratischer und bürgerrechtlicher IT überholen will ohne zuvor die Fehler der USA und Chinas gemacht zu haben: Die EU-Digitalstrategie erfolgt in einem demokratischen Prozess. Sie verfolgt zumindest in Ansätzen das Ziel „digitaler Souveränität", also den Abbau der Abhängigkeit von den USA und China. Mit der Datenschutz-Grundverordnung (DSGVO) hat Europa das globale Vorbild für digitalen Grundrechtsschutz entwickelt und als globalen „best standard" etabliert. Geht die EU einen „dritten Weg" mit ihrer Regulierung weiter, so kann sie nicht nur mehr Autarkie bei gleichzeitiger globaler Vernetzung erreichen, sondern auch eine globale grundrechtsorientierte Alternative zum privatwirtschaftlichen oder staatlichen Überwachungskapitalismus entwickeln.[3]

II Digitalstrategische EU-Regulierungen

Mit der Datenschutz-Grundverordnung (DSGVO) hat die EU in Sachen digitalem Grundrechtsschutz vorgelegt. Das Gesetz zu künstlicher Intelligenz (KI-Gesetz, AI-Act)[4] zielt auf Gemeinnützigkeit und Grundrechtsverträglichkeit, gepaart mit dem Anspruch der wirtschaftlichen Entfaltung des Potenzials von KI. Der Data Act (DA)[5] und der schon verabschiedete Data Governance Act (DGA)[6] sowie die geplanten neun Datenräume verfolgen ebenso gemeinnützige Anliegen. Der European Health Data Space (EHDS – Europäischer Gesundheitsdatenraum)[7] ist der erste ambitionierte spezifische Regelungsrahmen für die Primär- und Sekundärnutzung digitaler Daten.

Das Grundkonzept von DA, DGA und EHDS besteht hinsichtlich der Sekundärnutzung von Daten darin, dass der Dateninhaber, was wohl dem datenschutzrechtlichen Verantwortlichen entsprechen dürfte, verpflichtet wird bestimmte gemeinnützliche Daten zur Verfügung zu stellen (Art. 5 Abs. 1, 8 ff., 12 DA-E, Art. 3 Abs. 1 DGA, Art. 4, 33 Abs. 1 EHDS-E). Den Zugang hierzu können Nutzer von datengenerierenden Produkten einfordern (Art. 3 DA-E, Art. 3 EHDS-E). Vor allem wird Datenempfängern die Sekundärnutzung und damit die Weiterverwendung von Daten auf Antrag ermöglicht. Über den Zugang entscheiden neben den Dateninhabern nationale Zugangsstellen (Art. 36 ff. EHDS-E, Art. 7, 12 DGA: zuständige Stellen/Behörden). Der Datenaustausch erfolgt über spezifische Netzwerke der Datenräume, über Anbieter von Diensten für die gemeinsame Datennutzung (Art. 9 ff. DGA) und/oder über Verarbeitungsdienstleister (Art. 17 EHDS-E). Der Austausch, die Vermittlung und die Zusammenführung von Daten soll durch Interoperabilitätsstandards erleichtert werden (Art. 28 ff. DA-E, Art. 6, 23 EHDS-E). Eine zentrale Dateninfrastruktur soll den Überblick über verfügbare Daten und die Koordination von Prozessen gewährleisten (Art. 8 DGA; Art. 37, 52, 59 EHDS-E). Die Prozesse und die Organisation sind einer hoheitlichen Aufsicht unterworfen. Im Folgenden wird auf die jeweiligen Kommissionsentwürfe Bezug genommen bzw. beim DGA auf das schon verabschiedete, am 24.09.2023 in Kraft tretende Gesetz. Stellungnahmen und Ergänzungs- bzw. Gegenentwürfe von EU-Rat und Parlament bleiben hier im Interesse der Übersichtlichkeit unberücksichtigt.

III Der Paradigmenwechsel

Sämtliche Regulierungsvorschläge differenzieren wenig zwischen gemeinnützigen und (auch) privatnützigen Sekundärnutzungen. Was Gemeinnützigkeit ist, bleibt vage. So stehen in Art. 34 Abs. 1 EHDS-E die „wissenschaftliche Forschung im Bereich des Gesundheits- und Pflegesektors" ohne Unterscheidung neben „Entwicklungs- und Innovationstätigkeiten für Produkte und Dienste" oder „Training, Erprobung und Bewertung von Algorithmen". Für all diese Zwecke ist nicht nur eine Nutzungsmöglichkeit vorgesehen, sondern auch eine Bereitstellungspflicht der Dateninhaber (Art. 33 Abs. 1 EHDS-E). Hinter sämtlichen vorgesehenen Zwecken steht zwar irgendwie auch ein öffentliches Interesse, doch die Grenzen zwischen öffentlichen und privaten Nutzungsinteressen sind fließend. So gerät der mit der DSGVO intendierte Grundrechtsschutz in Gefahr – beim EHDS im hochsensitiven Bereich der Verarbeitung von Gesundheitsdaten.

Der Paradigmenwechsel vom Vorrang des individuellen Grundrechtsschutzes hin zur Nutzungserlaubnis bei Daten generell wie bei Gesundheitsdaten speziell ist angesichts der Notwendigkeiten und Potenziale im öffentlichen Interesse nicht zu verhindern und im Grundsatz zu begrüßen. Die Daten können die Grundlage für die Bewältigung dringender Aufgaben sein: Arbeitsschutz und Gesundheitsprävention, politische, ökologische und ökonomische Planung, Aus- und Fortbildung, Entwicklung und Bereitstellung von lebensnotwendigen Produkten und Diensten. Die DSGVO liefert für diese Zwecke allgemeine Rechtsgrundlagen. Sie erlaubt die Verarbeitung für berechtigte Interessen, soweit Grundrechtsinteressen nicht überwiegen (Art. 6 Abs. 1 lit. f), und wenn es um den Schutz lebenswichtiger (Art. 6 Abs. 1 lit. d) oder sonstiger öffentlicher Interessen (Art. 6 Abs. 1 lit. e) geht. Die Bereitstellung personenbezogener Daten für gemeinnützige Zwecke ist in unserer digitalisierten Gesellschaft nicht nur naheliegend, sondern zwingend, wenn angesichts der Risiken für Gesundheit, Umwelt, Klima, Ernährung, Unterbringung, soziale Absicherung Vorkehrungen und Schutzmaßnahmen getroffen werden sollen. Zumeist sind hierfür nur aggregierte Ergebnisse notwendig. Diese nicht mehr personenbezogenen Ergebnisse sind aber oft nur über personenbeziehbare Daten zu erlangen.

Die rechtlichen Vorgaben für den Ausgleich zwischen individuellem Schutzinteresse und Nutzungsinteresse finden wir in der DSGVO in Form von Garantien und Maßnahmen: Pseudonymisierung, Datensparsamkeit, Zweckbindung, Verschlüsselung, technisch-

organisatorische Maßnahmen, Folgenabschätzung, Transparenz, Betroffenenrechte. Diese Datenschutzmaßnahmen bleiben in der DSGVO allgemein. Sie müssen gemäß den jeweiligen Zwecken und Risiken unterschiedlich ausgestaltet werden, um adäquaten Grundrechtsschutz zu gewährleisten. Die neuen EU-Digitalregelungen müssten insofern die DSGVO präzisieren. Stattdessen erfolgt sehr weitgehend nur eine pauschale Verweisung auf die DSGVO und die dort vorgesehenen Instrumente oder deren inhaltliche Wiederholung (Art. 1 Abs. 3, 31 Abs. 2 DA-E, Art. 33 DGA, z.B. Art. 3 Abs. 3, 7, 9, 21 EHDS-E).

IV Forschungsregelungen

Die DSGVO vollzieht teilweise den Paradigmenwechsel vom Schutzkonzept zur Nutzungserlaubnis, indem sie die Nutzung „für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke" privilegiert, soweit hinreichende Schutzvorkehrungen gemäß Art. 89 Abs. 1 getroffen werden (Art. 5 Abs. 1 lit. b). Auch in Bezug auf die Betroffenenrechte erfolgt unter den gleichen Voraussetzungen eine Privilegierung (Art. 89 Abs. 2, 3 DSGVO).

Eine Relativierung der eigenen Vorgaben nimmt die DSGVO dadurch vor, dass sie den nationalen Gesetzgebern im Forschungsbereich über sog. Öffnungsklauseln weite Regelungsspielräume überlässt. Dieses Feld hatten die deutschen Gesetzgeber in Bund und Ländern lange vor dem Wirksamwerden der DSGVO bestellt. Und sie sahen in der DSGVO keinen bzw. wenig Anlass für eine Umsetzung des vorgezeichneten Paradigmenwechsels: Forschungsdatennutzungen werden weitgehend von der Betroffeneneinwilligung abhängig gemacht, unterliegen oft einer projektbezogenen Zweckbindung und sind von weiteren komplizierten Verfahrensvorgaben abhängig. Ein Flickenteppich verschiedener und sich teilweise widersprechender Regelungen macht es institutionen- und disziplinübergreifender Forschung oft praktisch unmöglich allen rechtlichen Anforderungen zu genügen. Ergebnis sind Forschungsbehinderungen und Einschränkungen. Alle Versuche, diesen Zustand auf nationaler Ebene zu verbessern, waren erfolglos, nicht zuletzt wegen den zwischen Bund- und Ländern aufgeteilten Gesetzgebungskompetenzen.[8]

Über eine verbindliche europaweite Regelung könnte eine Harmonisierung des Forschungsrechts – damit auch in Deutschland – erreicht werden. Die EU hat sich dieser Aufgabe mit ihren Regulierungsplänen gestellt, indem sie die Sekundärnutzung von Daten und „Datenaltruismus" (Art. 15 ff. DGA, Art. 40 EHDS-E) regelt und explizite gesetzliche Grundlagen schafft, welche nationale Regelungen ersetzen können. Bzgl. des Datenaltruismus ist zudem vorgesehen, dass Daten auch auf Einwilligungsbasis nach einem einheitlichen Format beschafft werden können (Art. 22 DGA), was für die Forschung aber keine grundlegende Verbesserung bedeutet. Es hätte nahegelegen insbesondere den von der DSGVO privilegierten Forschungsbereich näher zu normieren. Doch das ist bisher unterblieben. Zwar wirbt die EU für ihr Regelungskonzept immer wieder mit Erleichterungen für die wissenschaftliche Forschung.[9] Doch spielt die Forschung tatsächlich in den Regelungen keine prominente Rolle und wird weitgehend wie andere Zwecke behandelt.

V Europarechtliche Grundlagen

Dies ist irritierend, zumal die EU immer wieder behauptet in besonderem Maße die Grundrechte zu wahren. Das Trainieren von Algorithmen oder das Entwickeln von Produkten und Dienstleistungen kann – allenfalls indirekt und abgeleitet – keinen besonderen Grundrechtsschutz für sich in Anspruch nehmen und ist kaum in der Lage das Grundrecht auf Datenschutz, das in Art. 8 Grundrechte-Charta (GRCh) gewährleistet wird, zu verdrängen. Art. 13 GRCh sichert demgegenüber ausdrücklich die Forschungsfreiheit. Dieser Unterschied hinsichtlich der Wertigkeit bei der Zweitverwertung von (personenbezogenen) Daten muss sich in der Gesetzgebung widerspiegeln.

Die Gesetzgebungsorgane der EU sind daher gut beraten ausdrückliche und spezifische Forschungsdatennutzungsnormen vorzusehen. Gesetzessystematisch gehören diese Regeln in den allgemeinen Data Act (DA), eventuell auch in den – „Datenaltriusmus" spezifizierenden – Data Governance Act (DGA) und, soweit spezifische Normen für Gesundheitsforschung sinnvoll bzw. nötig sind, in den European Health Data Space (EHDS). Im Interesse einer europaweiten Harmonisierung und der Ermöglichung europäischer Forschung sollte eine weitgehend direkt anwendbare und abschließende Normierung erfolgen, die den nationalen Gesetzgebern nur Spielräume bei der Festlegung der Zuständigkeiten und der Spezifizierung der nationalen Verfahren eröffnet.

Spezifisches Forschungsrecht enthält nur Art. 21 DA-E, der öffentlichen Stellen, die im Rahmen „außergewöhnlicher Notwendigkeiten" von Dateninhabern „Notstandsdaten" erlangt haben, die Befugnis erteilt mit diesen forschen zu dürfen.

Teilweise wird die Gesetzgebungskompetenz der EU im Forschungsbereich in Frage gestellt. Tatsächlich hat die EU z.B. im Gesundheitsbereich gemäß Art. 168 Vertrag über die Arbeitsweise der EU (AEUV) nur eine subsidiäre Zuständigkeit. Soweit EU-Regelungen in die nationale Organisationshoheit eingreifen und nicht der Kooperations- und der Harmonisierungsaspekt für den Binnenmarkt (Art. 114 AEUV) im Vordergrund stehen, ist die Kompetenzfrage relevant. Bezieht sich ein Regelungsansatz auf Fragen des Datenschutzes und erfolgt so eine Konkretisierung der DSGVO, so besteht unzweifelhaft gemäß Art. 16 AEUV eine Zuständigkeit der EU. Zudem hat die EU gemeinsam mit den Mitgliedsstaaten gemäß Art. 173 Abs. 1, 179 AEUV die Pflicht und Aufgabe Forschung und technologische Entwicklung zu fördern.

VI Anforderungen an Datenzugänge für die Forschung

Eine zentrale Aufgabe eines Gesetzes ist es zu definieren, was unter dem Begriff „Forschung" geregelt wird, womit zugleich eine Präzisierung des Forschungsgrundrechts in Art. 13 GRCh einhergeht. Nicht jede erkundende Tätigkeit kann den Schutz des Art. 13 GRCh für sich in Anspruch nehmen, schon gar nicht, wenn damit einwilli-

gungsfrei Eingriffe in das Grundrecht auf Datenschutz legitimiert werden sollen. Bisher gibt es hierzu keine verbindlichen Festlegungen und auch noch keine konsistente Rechtsprechung des Europäischen Gerichtshofes (EuGH). Zurückgegriffen werden kann und sollte insofern auf die Definition des deutschen Bundesverfassungsgerichts. Forschung ist danach ein ernsthafter planmäßiger, auf wissenschaftlicher Eigengesetzlichkeit (Methodik, Systematik, Beweisbedürftigkeit, Nachprüfbarkeit, Kritikoffenheit, Revisionsbereitschaft) beruhender Prozess zum Auffinden von neuen Erkenntnissen, ihrer Deutung und ihrer Weitergabe.[10] Projekte, die dieser Definition nicht genügen, können keinen Anspruch auf personenbezogene Daten für sich geltend machen, ohne dass zuvor von den Betroffenen eine ausdrückliche und informierte Einwilligung eingeholt wurde.

Eingriffslegitimierend können nur Forschungsvorhaben sein, an denen ein öffentliches Interesse besteht. Ausschließlich private Interessen an einem Projekt können informationelle Eingriffe bei Betroffenen nicht legitimieren. Von der Forschungsprivilegierung nicht mit umfasst sein können daher Projekte im Bereich der Markt- und Meinungsforschung oder im Rahmen der Erforschung und Weiterentwicklung von Marktprodukten, an denen kein besonderes öffentliches Interesse besteht. Das öffentliche Interesse am Forschungsergebnis muss ausdrücklich formuliert und festgestellt sein. Ändert sich im Laufe eines Projektes der gemeinwohlorientierte Zweck, so ist dies nicht schädlich, doch muss dieser erneut klar definiert werden und überprüfbar sein.[11]

Die Definition von privilegierter Forschung kann nicht von deren Art der Finanzierung abhängig gemacht werden; diese kann öffentlich oder privat erfolgen. Es sollte für den Datenzugang keine Rolle spielen, ob es sich bei der forschenden Einrichtung um eine öffentliche Stelle (z.B. eine Universität oder Behörde) handelt oder um ein Privatunternehmen. Wohl aber muss gewährleistet sein, dass die Forschung unabhängig und ergebnisoffen erfolgt. Reine Auftragsforschung mit der Zielsetzung der Bestätigung vorgegebener Resultate ist ebenso auszuschließen wie die direktive externe Festlegung der wissenschaftlichen Abläufe und Ergebnisse.

Wissenschaftliche Forschung setzt den Einsatz wissenschaftlicher Methoden voraus, die geeignet sind einer neuen „Wahrheit“ möglichst nahe zu kommen. Es gibt nicht „eine“ Methode; die Methoden zur Erlangung wissenschaftlicher Erkenntnis stehen in einem pluralen Wettbewerb. Gemein muss ihnen sein, dass sie rational abzuleiten und hinterfragungsfähig und von der Wissenschaftsgemeinschaft als solche anerkannt sind. Projekte genügen dann den Ansprüchen an ein – Eingriffe legitimierendes – öffentliches Interesse, wenn bei ihnen eine valide wissenschaftliche Methode zur Anwendung kommt.

In Art. 15 ff. DGA sind datenaltruistische Organisationen geregelt. Hierbei muss es sich nicht, kann es sich aber um Forschungseinrichtungen handeln. Der Datenzugang für Forschungszwecke darf nicht auf solche Einrichtungen beschränkt sein, da das Forschungsgrundrecht grundsätzlich Jedermann zusteht. Wohl aber ist es möglich den Zugangsprozess für altruistische Organisationen zu erleichtern, die in einem vorgelagerten Verfahren ihre altruistische Zielsetzung und ihre Vertrauenswürdigkeit nachgewiesen haben. Das Forschungsgrundrecht für Jedermann begründet noch längst nicht für Jedermann einen Anspruch auf den Zugang zu Forschungsdaten. Diesen verdient nur, wer hierfür die Qualifikation nachweisen kann und sich der öffentlichen Kontrolle unterwirft.

Zur Dokumentation der konkret geplanten Durchführung der Datenverarbeitung muss jedem Forschungsprojekt ein Datenschutzkonzept zur Pflicht gemacht werden. Hierbei müssen – ähnlich einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) – die Prozesse, Risiken und zu ergreifenden Maßnahmen dargestellt werden.

Zu den Charakteristika wissenschaftlicher Forschung gehört, dass sie hinsichtlich des Forschungsdesigns und der dabei erfolgenden Datenverarbeitung offen für Hinterfragung und Kritik ist. Dies setzt Transparenz voraus. Transparenz ist in Bezug auf die datenschutzrechtlich Betroffenen nötig. Diese lässt sich über Internetportale verwirklichen, soweit nicht eine individuelle Information und Ansprache angezeigt und möglich ist. Transparenzbedarf besteht auch gegenüber der allgemeinen und wissenschaftlichen Öffentlichkeit, die im demokratischen Diskurs die Gemeinwohlorientierung und Verhältnismäßigkeit zu hinterfragen in der Lage ist (Art. 18 DGA zu datenaltruistischen Organisationen). Die Transparenzpflicht gebietet es nicht das gesamte Vorgehen in einem Projekt offenzulegen. Vielmehr muss die Logik des Projektes und das Ergebnis plausibel nachvollziehbar sein; nicht offenbart werden müssen Betriebs- und Geschäftsgeheimnisse, die für die Plausibilitätsprüfung nicht benötigt werden.

Die Veröffentlichung der erlangten Erkenntnisse ist ein zentraler Bestandteil des wissenschaftlichen Dialogs, wodurch die Ergebnisse auf ihre Richtigkeit hin überprüft werden können. Aufbauend auf die gefundenen Ergebnisse können weitere Erkenntnisse gesucht werden. Forschung ist letztlich auf Kommunikation und Publikation ausgerichtet (vgl. Art. 179 Abs. 1 AEUV). Die kommunikative Rolle der Forschung spiegelt sich in der Regelung des Art. 85 DSGVO wider, der die wissenschaftlichen Zwecke in den Regelungsbereich „Meinungsäußerung und Informationsfreiheit“ einordnet. Forschung mit auf gesetzlicher Grundlage erlangten Daten ist in besonderem Maße rechenschaftspflichtig. Hierfür muss eine Offenlegung der Ergebnisse innerhalb einer angemessenen Frist zur Pflicht gemacht werden. So kann im Nachhinein überprüft werden, ob die Genehmigung des Datenzugangs materiell gerechtfertigt war. Bei zeitlich unbefristeten oder langjährigen Projekten können und sollten auch Zwischenberichte bzw. Evaluationen zur Pflicht gemacht werden.

Für den Datenzugang muss ein Genehmigungsverfahren vorgesehen werden. Im Nachhinein muss festgestellt werden, ob die Genehmigungsanforderungen eingehalten wurden. Erweist sich der Dateneinsatz in Bezug auf die Resultate als erforderlich und verhältnismäßig (allgemein Art. 8 Abs. 5 DA-E)? Wurden die wissenschaftlichen Standards eingehalten? Forschung ist ergebnisoffen und kann scheitern. Ein Scheitern macht die Datenverarbeitung nicht unzulässig, es

kann aber relevant für spätere Zugangsgenehmigungen sein.

Denkbar ist, dass zusätzlich zur Transparenz gegenüber der Öffentlichkeit und den Betroffenen vom Forschungsprojekt spezifische Transparenzpflichten gegenüber dem Dateninhaber oder -lieferanten eingegangen werden. Diese können in einer Rückspiegelung der durch das Projekt „veredelten" Daten bestehen oder in einer qualifizierten Berichterstattung über die Ergebnisse. Wurden verschiedene Datenquellen genutzt, so ist darauf zu achten, dass über diesen Umweg keine unzulässigen Datenübermittlungen und keine Vertraulichkeitsverletzungen erfolgen.

Die datenschutzrechtliche Privilegierung von Forschungszwecken hat zur Folge, dass eine strenge Zweckbindung gelten muss. Es ist auszuschließen, dass durch eine Weiterverwendung von Forschungsdaten die generell geltenden Zweckbindungsregelungen durchbrochen werden. Die strenge Zweckbindung dient dem Vertrauen in die Unabhängigkeit der Forschung und ist Kompensation für die Herausgabeverpflichtung der Dateninhaber. Die Zweckbindung muss auch gegenüber staatlichen Einrichtungen gelten. Es ist daher geboten ein Forschungsgeheimnis zu normieren, das ein Zeugnisverweigerungsrecht und ein Beschlagnahmeverbot einschließt. Die Zweckbindung muss auch innerhalb der verantwortlichen Stelle gewahrt bleiben, weshalb der organisatorische und personelle Rahmen des Forschungsprojektes präzise festzulegen ist. Die Wahrung der Vertraulichkeit dient nicht nur der Wahrung des Datenschutzes, sondern auch dem Schutz sonstiger immaterieller Rechte wie der Wahrung von Betriebs- und Geschäftsgeheimnissen und von Urheberrechten. Die Wahrung der Zweckbindung ist durch Sanktionsandrohungen im Fall des Verstoßes zu flankieren (Art.33 DA-E, Art. 31 DGA, Art. 43 EHDS-E). Diese Sanktionen müssen durch eine hinreichende Aufsicht und Kontrolle effektiv umsetzbar sein.

VII Datenzugangs-Verfahren

Ein Antrag auf Datenzugang muss das Vorliegen der o.g. Voraussetzungen nachweisen. Die angeforderten Daten müssen von Relevanz für die erforschte Fragestellung und die angestrebten, im Allgemeininteresse liegenden Ergebnisse und insofern verhältnismäßig sein.

Die Datenbereitstellung verursacht beim Dateninhaber Kosten, die diesem grundsätzlich zu ersetzen sind, was in der Regel dem Datennutzer auferlegt werden kann. Diese Kosten müssen angemessen und aufwandsbezogen sein (Art. 9 DA-E, Art. 6 DGA, Art. 42 EHDS-E). Gesetzlich ermöglichte spekulative Gewinne würden eine Forschungsbehinderung darstellen und können zu einer finanziellen Diskriminierung bestimmter Forschungsvorhaben führen.

Bei der organisatorischen Umsetzung der Datennutzungsinfrastruktur verweisen die EU-Regelungen weitgehend auf die nationalen Gesetzgeber (Art. 31 ff. DA-E, Art. 7 f., 12 DGA, Art. 36 EHDS-E). Damit sollte es nicht sein Bewenden haben. Um wirklich EU-weit Forschung zu fördern, bedarf es auch einer EU-weiten Infrastruktur (so Art. 52-54 EHDS-E).

Die europäischen Regulierungsvorhaben machen bisher keine forschungsspezifischen Aussagen zur Genehmigungsstelle, die den Zugang der Daten vom Dateninhaber für die Forschungseinrichtung prüft, genehmigt und herstellt (Art. 36 EHDS-E). Dadurch wird die Gefahr begründet, dass der Vertraulichkeit und der Integrität der Forschung nicht das nötige Vertrauen gezollt wird.

Die Genehmigung des Datenzugangs für Forschungszwecke sollte daher von sonstigen Daten-Zugangsgenehmigungen klar getrennt werden. Die verfassungsrechtliche Sonderstellung von Forschung muss sich im Genehmigungsprozess widerspiegeln. Zentral ist, dass die Genehmigungsstelle von ministeriell-exekutiven Interessen unabhängig ist. Zugleich sind spezifische Kenntnisse der wissenschaftlichen Forschung nötig; Interessenkonflikte mit dem Antragsteller müssen vermieden werden. Insofern bieten sich korporative Entscheidungsgremien an, in denen Sachverstand aus folgenden Bereichen nötig ist: Wissenschaft, Datenschutz, Ethik und Informatik (ähnlich Art. 36 Abs. 3 EHDS-E). Eine dezentrale Struktur mit einer starken Vernetzung sollte sichergestellt werden. Die Vernetzung zielt einerseits auf den Informationsaustausch untereinander ab wie auch auf die kollektive und gebündelte Informationsbereitstellung gegenüber den Betroffenen und der Öffentlichkeit.

Sämtliche EU-Gesetzespläne sehen eine staatliche Aufsicht vor (z.B. Art. 31 ff. DA-E). Dort können betroffene juristische oder natürliche Beschwerden vorgebracht werden (Art. 32 DA-E, Art. 24 DGA). Die Aufsichtsbehörden arbeiten zusammen; soweit Datenschutz Thema ist, sind die Datenschutzaufsichtsbehörden einzubeziehen (Art. 12 Abs. 3 DGA). Hinsichtlich einer staatlichen Aufsicht im Forschungsbereich bedarf es – zusätzlich zu der Genehmigung und Überwachung der konkreten Durchführung der Forschungsprojekte – einer unabhängigen Rechtsaufsicht sowohl über die Forschungsdatenverarbeitung als über das Handeln der Genehmigungsstellen (ähnlich Art. 23 DGA).

Die in den Regelungsvorschlägen der EU-Kommission weit verbreitete Unart, sich selbst die Befugnis zuzusprechen über „Delegated Acts" Präzisierungen der gesetzlichen Regelungen vorzunehmen (Art. 38 DA-E, Art.28 DGA, Art. 67 EHDS-E), ist generell zu hinterfragen. In jedem Fall darf sie bei der Forschungsregulierung nur sehr zurückhaltend zum Einsatz kommen. Forschung sollte so weit wie möglich staatsfern erfolgen – der Wahrheit und nicht einer Exekutive verpflichtet.

VIII Forschungsdatengesetz – Gesundheitsdatennutzungsgesetz

Die obigen Überlegungen zielen auf eine Ergänzung der bisherigen Vorschläge bzw. Regelungen der EU im Rahmen von deren Digitalstrategie. Sie sind auf die nationale Gesetzgebung übertragbar. Ob überhaupt und in welchem Umfang sich die EU der Forschungsthematik spezifisch annehmen wird, ist noch unklar. Unabhängig davon haben bis dahin die nationalen Gesetzgeber – auch in Deutschland – das Recht eigene Regelungen zu treffen. In jedem Fall sind die nationalen Gesetzgeber aufgefordert, wo das EU-Recht Regelungslücken lässt, diese zu füllen. Das nationale Recht sollte sich hinsichtlich Struktur, Zielsetzung und materieller Vorgaben an den bestehenden wie an den geplanten und absehbaren europäischen Vorgaben orientieren.

Die obigen Gesetzgebungsvorschläge für die EU eignen sich auch als Vorlage für nationales Recht, das schneller und weniger aufwändig geändert werden kann als in der EU. Im rot-grün-gelben Koalitionsvertrag haben die Regierungsparteien für die Legislaturperiode bis 2025 u.a. die Erarbeitung eines Forschungsdatengesetzes sowie eines Gesundheitsdatennutzungsgesetzes angekündigt.[12] Insofern lassen sich die obigen Ausführungen auf ein allgemeines Forschungsdatengesetz übertragen, die Ausführungen zum EHDS sind für ein Gesundheitsdatennutzungsgesetz übertragbar. Spezifische Aussagen zur Gesundheitsforschung lassen sich in jedem der beiden geplanten Gesetze realisieren.

Um den Konflikt zwischen Bundes- und Ländergesetzgebungskompetenz im Forschungsbereich aufzuheben, wäre eine Grundgesetzänderung wünschenswert. Sollte dies politisch nicht möglich sein, könnte der Bund eine Gesetzesregelung vorgeben, der sich die Länder anschließen können.

Intensiv diskutierte, erprobte und bewährte nationale Datenraumstrukturen und -normen können sich gegenseitig wie auch letztlich die europäische Regulierung inspirieren und Vorbild sein.

IX Fazit

Die Privatwirtschaft, insbesondere die Internetwirtschaft, hat den Paradigmenwechsel vom Schutz personenbezogener Daten zu deren Nutzung schon vor Jahren vollzogen und berücksichtigt hierbei die individuellen Datenschutzbedürfnisse unzureichend. Sie zeigt damit die Risiken, aber auch das Potenzial auf, das in der Nutzung personenbezogener Daten liegt. Dieses Potenzial im Interesse der Allgemeinheit zu heben muss das Anliegen der anstehenden europäischen Gesetze sein. Der grundsätzliche Ansatz ist insofern zu begrüßen. Die konkreten Regelungsvorschläge bleiben teilweise aber noch weit hinter einem angemessenen Grundrechtsschutz zurück.[13]

Dies gilt nicht nur für den Datenschutz, sondern auch für die Operationalisierung der Forschungsfreiheit. Forschung dient als eines der gängigsten Erklärungsmuster der neuen Gesetze, doch ist die normative Umsetzung hierzu bisher notleidend. Der vorliegende Beitrag dient dazu diese Defizite sowie Lösungsvorschläge aufzuzeigen. Es ist zu hoffen, dass die Vorschläge vom Rat und Parlament der EU aufgegriffen und in das Gesetzespaket eingeführt werden.

Die vorgeschlagenen EU-Regelungen zur Forschung wären in der Lage die gewaltigen Regelungsdefizite beim Datenschutz im Forschungsbereich auf nationaler Ebene zu überregeln und damit zu verdrängen. Sie sind geeignet einen grundrechtskonformen Forschungsdatenraum in Europa zu schaffen. Bis es soweit ist, werden noch Jahre vergehen. Daher ist der nationale Gesetzgeber gut beraten seine Bemühungen für ein Forschungsdatengesetz und für ein Gesundheitsdatennutzungsgesetz zu forcieren und – unter Beachtung der europäischen Pläne – umzusetzen. Damit könnte sich Deutschland an die Spitze einer Diskussion setzen, die darauf abzielt, dass Europa beim Datenschutz Spitze bleibt und bei der wissenschaftlichen Forschung wird.

1 Europäische Kommission, Eine europäische Datenstrategie v. 19.02.2020, COM(2020) 66 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

2 Koalitionsvereinbarung 2021-2015 der Parteien SPD, Bündnis 90/Die Grünen, FDP, abgedruckt in DANA 1/2022, 18 ff.

3 Weichert, Digitale Grundrechte im internationalen Kontext, DANA 3/2022, 142 ff.

4 Europäische Kommission, Vorschlag für ein Gesetz über Künstliche Intelligenz, v. 21.04.2021, COM(2021) 206 final, 2021/0106(COD).

5 Europäische Kommission, Vorschlag für ein Datengesetz v. 23.02.2022, COM(2022) 68 final, 2022/0047(COD).

6 Verordnung (EU) 2022/868 v. 30.05.2022, ABl. EU v. 03.06.2022, L 152/1.

7 Europäische Kommission, Vorschlag für einen Europäischen Raum für Gesundheitsdaten v. 03.05.2022, COM(2022) 197 final, 2022/0140 (COD); Bernhardt/Ruhmann/Weichert, DANA 1/2023, 17 ff.

8 Z.B. Krawczak/Weichert, Medizinforscher und Datenschützer fordern Bund-Länder-Staatsvertrag, DANA 4/2017, 193 ff.

9 Z.B. Europäische Kommission, Europäische Gesundheitsunion: Ein europäischer Raum für Gesundheitsdaten für Menschen und Wissenschaft, 03.05.2022, https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2711.

10 BVerfG 29.05.1973 – 1 BvR 424/71 u. 325/72, Rn. 128; Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, 18; ähnlich Art. 2 lit. b Richtlinie 2005/71/EG des Rates über ein besonderes Zulassungsverfahren für Drittstaatsangehörige zum Zweck der wissenschaftlichen Forschung v. 12.10.2005.

11 Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, 110 f.

12 Koalitionsvertrag (En. 2) S. 21, 83, abgedruckt in DANA 1/2022, 20 f.

13 In die richtige Richtung geht der Entwurf eines Berichts des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments v. 10.02.2023, 2022/0140(COD).

Achim Klabunde

Gefahr für das Kommunikationsgeheimnis? Kein Fortschritt bei der ePrivacy-Verordnung

Nach der Verabschiedung der DSGVO legte die Europäische Kommission den Entwurf einer Verordnung zum Schutz der Kommunikation (ePrivacy-VO) im Januar 2017 vor, das Europäische Parlament (EP) verabschiedete seine Verhandlungsposition mit Änderungsanträgen noch im selben Jahr. Der Ministerrat (Rat) brauchte bis zum Jahr 2021, um sich auf eine Position zu einigen. Seitdem laufen Verhandlungen zwischen EP und Rat. Auf Seite des Rats verhandelt eine Delegation der Mitgliedsstaaten unter Führung der Ratspräsidentschaft.

Die EP-Berichterstatterin Birgit Sippel reagierte auf die Ankündigung der Präsidentschaft: „Die Schwedische Ratspräsidentschaft zeigt sich – so wie ihre Vorgängerinnen – sehr interessiert an allen digitalen Dossiers, die die Nutzung von Daten für wirtschaftliche Zwecke oder den Zugang zu personenbezogenen Daten für den Schutz der öffentlichen Sicherheit zum Ziel haben. Aber die Absage der ePrivacy-VO-Verhandlungen von Seiten der Schwedischen Ratspräsidentschaft zeigt: Beim Schutz der Bürgerinnen und Bürger vor Überwachung und Vertraulichkeit der Kommunikation hört das Interesse an Fortschritt auf. Doch statt sich klar zu positionieren schiebt die Ratspräsidentschaft das unliebsame Dossier nach hinten – ohne deutlich zu machen, wie sie Privatsphäre und Vertraulichkeit der Kommunikation anders sichern will. Digitale Grundrechte werden damit von den Mitgliedsstaaten auf das Abstellgleis verlegt."

Zu den von der schwedischen Präsidentschaft vorangetriebenen Vorhaben gehört natürlich auch die als „Chatkontrolle" bekannt gewordene Initiative eine vorsorgliche Überwachung von Kommunikation zur angeblichen Verhinderung und Bekämpfung von Kindesmissbrauch zu ermöglichen (CSAM). Ironischerweise ist die einzige zwischen Rat und Parlament bisher erzielte Einigung eine Sonderregelung, die den Plattformbetreibern erlaubt freiwillige Überwachungsmaßnahmen, die der ePrivacy-Richtlinie eigentlich zuwiderlaufen, zum Schutz von Kindern fortzusetzen. Die Zivilgesellschaft hat vielfach darauf hingewiesen, dass der unter dem Stichwort CSAM geforderte Zwang zur Chatüberwachung eine Vorratsdatenspeicherung unter einem anderen Namen darstellt und damit die gleichen Grundrechtsverstöße umfasst wie diese.

Sofern es keine Einigung im gegenwärtigen Verfahren zur ePrivacy-VO gibt, bleibt die bisherige Richtlinie in Kraft. Dazu meint Frau Sippel: „Die ePrivacy-Richtlinie, die vor über 20 Jahren in Kraft getreten ist, leistet weiterhin noch gute Dienste – insbesondere im Zusammenhang mit Vorschriften zur Vorratsspeicherung bei der Interpretation durch den Europäischen Gerichtshof. Mit der Richtlinie haben wir 27 verschiedene Interpretationen und Anwendungen der Bestimmungen in nationalen Gesetzen. Die Rechtsdurchsetzung steht vor großen Herausforderungen und hapert gewaltig. Unabhängig davon, dass bisher immer noch nicht alle Mitgliedsstaaten die Richtlinie vollständig und korrekt umgesetzt haben, liegen die Vorteile der Verordnung insbesondere darin, dass wir den Anwendungsbereich deutlich erweitern und wichtige Schutzlücken im Zusammenhang mit der alltäglichen Nutzung von sog. ‚OTT' wie Messengern und E-Mail-Diensten schließen könnten. Aus meiner Sicht verpassen wir als Europäische Gesetzgeber damit die einmalige Chance die Grundrechte der Europäerinnen und Europäer zu stärken, wenn die ePrivacy-Verordnung keine Realität wird."

Heinz Alenfelder

BigBrotherAward-Verleihung 2023 – Ein Großereignis

Anlässlich der Verleihung der deutschen BigBrotherAwards (BBA) haben wir 2022 an dieser Stelle die Hintergründe der „Oscars für Datenkraken" sowie die Gewinner und Eindrücke von der Gala aufgeführt (DANA 2/2022, 92 f.). Deshalb dokumentieren wir heute nur kurz und knapp die Preisträger 2023 und erklären, warum es sich bei der Gala zur Verleihung der BBA mittlerweile um ein Großereignis handelt.

Die Jury bestand wie im letzten Jahr aus Frank Rosengart (Chaos Computer Club), padeluun (Digitalcourage), Peter Wedde (Professor für Arbeitsrecht und Recht der Informationsgesellschaft), Rena Tangens (Digitalcourage) und Thilo Weichert (DVD und Netzwerk Datenschutzexpertise). Ausführlichere Informationen über die Jury und auch die Laudationes finden sich auf der Webseite www.bigbrotherawards.de.

In diesem Jahr lauteten die Preiskategorien: Behörden und Verwaltung, Fi-



Bild: Inflac

nanzen, Kommunikation, Verbraucherschutz und Lebenswerk:

- Das Bundesfinanzministerium erhält als Behörde den Preis für das seit Anfang des Jahres geltende Plattformen-Steuertransparenzgesetz (PStTG), welches Plattformanbieter u.a. zur umfassenden Vorratsdatenspeicherung über private „Flohmarktverkäufe" zwingt.
- In der Kategorie Finanzen erhält das Fintech-Unternehmen finleap den Preis dafür, dass es über Jahre hinweg fälschlicherweise Informationen zum Kontowechsel an Firmen schickt, die mit dem Vorgang nichts zu tun haben.
- Der Preis in der Kategorie Kommunikation geht an Zoom Video Communications Inc., die als US-Unternehmen Daten an Geheimdienste weiterleiten muss, aber dennoch behauptet DS-GVO-konform zu sein.
- Die Deutsche Post DHL Group erhält den Preis in der Kategorie Verbraucherschutz für praktizierten Digitalzwang. Sie will die Kunden und Kundinnen durch die Umstellung (der Funktionsweise) ihrer Packstationen dazu zwingen ein Smartphone und ihre Post & DHL-App zu nutzen. Dieser Digitalzwang gehört besonders gerügt, denn hier schließt ein ehemaliges Staatsunternehmen Bürgerinnen und Bürger (ohne Smartphone und App) von einer wichtigen Grundversorgung aus.
- Für das Lebenswerk laudatierte schließlich Thilo Weichert Microsoft dafür, dass es mit seiner Marktmacht Menschen, Unternehmen und Behörden zwingt bei deren digitalen Aktivitäten dauernd Daten in die USA zu übermitteln und sich dadurch in Echtzeit überwachbar zu machen. Damit wird Microsoft bereits zum zweiten Mal (zuerst im Jahr 2002) in der Kategorie Lebenswerk ausgezeichnet.

Die diesjährige, wiederum aufwändig organisierte Gala zur Verleihung der BBA fand durch Streaming als Großereignis in vielen Städten der Bundesrepublik gleichzeitig statt. Laut der Übersicht auf der o.a. Webseite organisierten Digitalcourage-Orts- und Hochschulgruppen von Kiel und Bremen über Leipzig und Köln bis Bayreuth – um nur einige herauszugreifen – jeweils ein Public Viewing. Auch andere Vereine wie der Hackspace Mudbyte e.V. aus Marburg oder der Förderverein Freifunk im Neanderland e.V. hatten zum gemeinsamen Treffen eingeladen, wohl nicht zuletzt, um die eigene Arbeit bekannter zu machen. Es ist anzunehmen und zu hoffen, dass die Fan-Gemeinde der deutschen BigBrotherAwards in den nächsten Jahren weiter wächst und der Intention der Preisverleihung zu einer immer größeren Stärke verhilft.

Sakyi Mannah

Ermächtigung zum Einsatz der Polizeisoftware hessenDATA ist verfassungswidrig

Sowohl in Hessen als auch in Hamburg sollten mithilfe der sog. „Polizeisoftware" hessenDATA präventiv Straftaten verhindert werden. Das Bundesverfassungsgericht urteilte nun über die am 2. Juli 2019 und 20. November 2020 eingegangenen Verfassungsbeschwerden, in denen die Beschwerdeführenden den § 25a des Hessischen Sicherheits- und Ordnungsgesetzes (HSOG) und den § 49 des Gesetzes über die Datenverarbeitung der Polizei des Landes Hamburg (HmbPolDVG) rügten, welche als Ermächtigungsgrundlagen zum Einsatz von hessenDATA dienten (BVerfG Urteil vom 16. Februar 2023 - 1 BvR 1547/19). Die Beschwerdeführenden trugen in beiden Verfahren vor, dass die Gesetze verfassungswidrig seien und sie durch die dadurch legitimierten Eingriffe in ihrem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), dem Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13

Abs. 1 GG), dem Fernmeldegeheimnis nach Art. 10 Abs. 1 GG und dem Grundrecht auf effektiven Rechtsschutz aus Art. 19 Abs. 4 GG verletzt würden.

Das Bundesverfassungsgericht bejahte in seinem Urteil am 16. Februar 2023 die Verfassungswidrigkeit beider Gesetze mit der Begründung, dass die verfassungsrechtlichen Anforderungen an die Rechtfertigung einer automatisierten Datenanalyse oder -auswertung nach der konkreten Ausgestaltung des § 25a HSOG und des § 49 HmbPolDVG schärfer und strenger sind als bei einer einfachen weiteren Nutzung der Daten. Insbesondere die datenschutzrechtlichen Grundsätze der Zweckbindung und Zweckänderung waren hierbei bedeutend. Die Befugnisse zur Abwehr von Gefahren nach § 25a Abs. 1 Alt. 2 HSOG und § 49 Abs. 1 Alt. 2 HmbPolDVG, so erklärte das Gericht, blieben jedoch unberührt.

Dieses Urteil stellt klar, dass derartige KI-basierten polizeilichen Informationssysteme nicht per se verboten sind. Vielmehr schafft das Urteil Rechtssicherheit betreffend die Speicherung und die nachgelagerten Datenanalysen in solchen Systemen, welche intensivere Grundrechtseingriffe darstellen könnten als gewöhnliche Verarbeitungen personenbezogener Daten.

Das Gericht erklärte in seinem Urteil, dass je weiter die automatisierte Weiterverarbeitung von Daten bei einer Datenanalyse oder -auswertung reiche, umso mehr entferne sich der darin liegende Eingriff von der ursprünglichen Datenerhebung. Dies habe allerdings zur Folge, dass der Grundsatz der Zweckbindung nicht mehr ausreiche, um die erneute Datenverarbeitung verfassungsrechtlich zu rechtfertigen. Für diese sog. Zweckänderung bedürfe es folglich einer weiteren datenschutzrechtlichen Rechtsgrundlage, welche die Weiterverarbeitung rechtfertige.

Werden durch die automatisierte Auswertung der Daten nicht nur die in den Daten angelegten, sondern mittels Verknüpfung der Daten auch verborgene Erkenntnisse über einzelne Personen gezogen und so nutzbare Profile einer Person erstellt, könnte sich dieser Vorgang bei einem entsprechenden Einsatz der Plattform dem sog. „Profiling" i.S.d. Art. 22 DSGVO annähern.

Die durch das Urteil klargestellten Anforderungen an KI-basierte Datenverarbeitungen im Kontext polizeilicher Gefahrenabwehr könnten zudem auch für andere – möglicherweise privatrechtlich organisierte – KI-basierte Plattformen und Datenverarbeitungen eine hohe Relevanz erhalten. Thematisch ebenfalls zumindest im erweiterten Kontext der Gefahrenabwehr bzw. Daseinsvorsorge betätigen sich etwa auch Krisenresilienzplattformen wie z.B. die Cognitive Economy Intelligence Plattform für die Resilienz wirtschaftlicher Ökosysteme (CoyPu). Auch für diese Plattformen wird mit hoher Wahrscheinlichkeit die Verarbeitung von personenbezogenen Daten eine sehr wichtige Rolle spielen.

(Der Beitrag stellt die persönliche Auffassung des Autors dar und ist im Rahmen des vom Bundesministerium für Wirtschaft und Klimaschutz geförderten Forschungsprojektes Cognitive Economy Intelligence Plattform für die Resilienz wirtschaftlicher Ökosysteme – CoyPu, https://coypu.org – entstanden; zu dem Urteil siehe auch die Darstellung in diesem Heft S. 113)

Presseerklärung der Deutschen Vereinigung für Datenschutz e.V. (DVD) vom 27.02.2023

Sachsen-Anhalt: DVD warnt vor Vetternwirtschaft beim Datenschutz

Mit Entsetzen verfolgt die Deutsche Vereinigung für Datenschutz e.V. (DVD) seit langem die Diskussion über den Datenschutz in Sachsen-Anhalt, die nun mit einem abgekarteten Prozess zur Besetzung der Stelle des Landesbeauftragten fortgesetzt wird. Diese ist seit über zwei Jahren vakant. Zuvor war Harald von Bose zwei Jahre länger als gesetzlich vorgesehen im Amt. Mit einer Gesetzesänderung und einer fragwürdigen Personalrochade soll nun offenbar ein CDU-Abgeordneter auf diesen Posten gehievt werden.

Im Oktober 2022 scheiterte die Wahl des von der Regierung vorgeschlagenen Kandidaten Albert Cohaus, der das Amt weiterhin kommissarisch wahrnimmt, dadurch, dass große Teile der regierenden CDU-Fraktion ihm die Stimme mehrfach verweigerten. Die CDU-Abgeordneten stimmten dem anerkannten Datenschützer Cohaus nicht zu, weil sie offenbar einem Abgeordneten aus den eigenen Reihen diesen Posten zuschachern wollen. Dem dient ein Gesetzesvorschlag der Regierungsfraktionen, der den Fraktionen ein Vorschlagsrecht zuspricht und die gesetzliche Verpflichtung zur öffentlichen Ausschreibung aufhebt (LT-Drs. 8/2255 v. 16.02.2023). Vorausgegangen war eine Absprache der Regierungsfraktionen, wonach die SPD den Vizepräsidenten des Landesrechnungshofs, die FDP die Vizepräsidentin des Landesverwaltungsamtes und die CDU den Datenschutzbeauftragten benennen darf.

Die DVD hat Hinweise darauf, dass mit dieser Abrede eine dubiose Personalrochade durchgeführt werden soll, mit der dem bei der Landtagswahl gescheiterten CDU-Nachrücker Arnd Czapeck wieder ein Landtagsmandat beschafft werden soll. Czapeck wurde im Zusammenhang mit der Beantragung von Fluthilfegeldern wegen Betruges zu einer Freiheitsstrafe von acht Monaten auf Bewährung

verurteilt. Er soll offenbar durch das Nachrücken mit Landtagsdiäten aus seiner prekären finanziellen Situation befreit werden. Hierfür müsste ein CDU-Abgeordneter zum Datenschutzbeauftragten gewählt werden und dadurch aus dem Landtag ausscheiden. Dieser Vorgang soll nach Verabschiedung der nun geplanten Gesetzesänderung über die Bühne gehen.

Die DVD weist darauf hin, dass ein solches Vorgehen schlicht unzulässig und ein Bärendienst für den Datenschutz und das Land Sachsen-Anhalt wäre: Die bisherige Regelung im Datenschutzgesetz des Landes, wonach die Stelle des Datenschutzbeauftragten öffentlich auszuschreiben ist, entspricht den Vorgaben der DSGVO. Nach diesen muss die Besetzung „im Wege eines transparenten Verfahrens“ erfolgen. Für die Stelle kommt nur eine Person in Frage, „die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten“ verfügt (Art. 53 DSGVO).

DVD-Vorstandsmitglied Thilo Weichert: „Wir kennen keinen CDU-Abgeordneten, der die europarechtlich geforderten Voraussetzungen erfüllt. Das anscheinend geplante Vorgehen ist nicht transparent, sondern Ausdruck übler Vetternwirtschaft. Es wäre für den Datenschutz in Sachsen-Anhalt eine Katastrophe, wenn er auf diese Weise weiter heruntergewirtschaftet würde.“

DVD-Vorsitzender Frank Spaeing ergänzt: „Nicht nur die Abgeordneten der CDU, sondern sämtliche Parlamentarier, insbesondere der Regierungsfraktionen, sind gut beraten beim geplanten Stühlerücken nicht mitzumachen. Nötig ist eine öffentliche Ausschreibung. Die CDU-Fraktion kann gerne jemand aus ihren Reihen zur Bewerbung auffordern. Die qualifizierteste Kandidatin oder der qualifizierteste Kandidat sollte ausgewählt werden.“



Nachruf auf Spiros Simitis – Ende einer Ära

Am 18. März 2023 ist Prof. Dr. Dr. h.c. mult. Spiros Simitis verstorben. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) trauert um einen der Begründer und Gestalter des Datenschutzes in Deutschland und Europa. Mit ihm verliert der Datenschutz einen eloquenten Fürsprecher und zugleich einen feinsinnigen und klugen Verteidiger, der neugierig und versiert neue Entwicklungen aufgriff und konstruktiv weiterdachte. Grieche von Geburt, Europäer aus Überzeugung und Datenschützer aus Leidenschaft.

In seiner Person vereinte Spiros Simitis Wissenschaft und Praxis des Datenschutzes. Er war seit 1969 als Professor für Arbeitsrecht, Bürgerliches Recht und Rechtsinformatik in Frankfurt am Main insbesondere mit arbeitsrechtlicher Perspektive ein Vordenker des Datenschutzes und unterstützte bei der Erarbeitung des ersten Datenschutzgesetzes der Welt, des hessischen Datenschutzgesetzes von 1970. Von 1975 bis 1991 war er Hessischer Datenschutzbeauftragter und setzte sein Wissen und seine Überzeugungskraft für die Sicherstellung von Datenschutz in der Anwendung ein. Sein gewinnendes Auftreten machte ihn zu einem gefragten Gesprächspartner und Berater im In- und Ausland. Im Rahmen des Europarates sowie als Berater der EU-Kommission nahm Spiros Simitis erheblichen Einfluss auf die Fundierung des Datenschutzes in Europa. Er trug wesentlich dazu bei die Grundlagen zu legen, auf denen das Datenschutzrecht bis heute und in Zukunft aufbaut.

Spiros Simitis setzte sich auch nach seiner Emeritierung weiter mit großem Geschick und intellektueller Brillanz für den Schutz des Rechts auf informationelle Selbstbestimmung ein. In zahlreichen Publikationen und führenden Kommentierungen, aber auch in effektiver Politikberatung wirkte er stetig an der Fortentwicklung des Datenschutzrechts mit. Mit ihm endet eine Ära des Neuaufbaus des Datenschutzrechts mit dem Schaffen von Grundlagen; spätestens seit Geltung der Datenschutz-Grundverordnung ist der Datenschutz im Kern jeglicher Digitalisierung und in der Mitte der Gesellschaft angekommen.

Zum Vermächtnis von Spiros Simitis gehört es unter den Bedingungen sich dynamisch entwickelnder Informations- und Kommunikationstechnologien die Freiheit der Einzelnen durch Recht zu sichern. Die Datenschutzkonferenz sieht sich diesem Vermächtnis verpflichtet. Im Geiste von Spiros Simitis wird sie die Rechte und Freiheiten und insbesondere die informationelle Selbstbestimmung der Bürgerinnen und Bürger schützen, verteidigen und weiterentwickeln.

Wir werden Spiros Simitis vermissen.

(Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 21.03.2023)

Öffentlicher Brief aus der Zivilgesellschaft zum Vorschlag eines französischen Gesetzes über die Olympischen Spiele und die paralympischen Spiele 2024

01.03.2023

Sehr geehrte Abgeordnete der Nationalversammlung,

Wir, die unterzeichnenden 37 zivilgesellschaftlichen Organisationen, bringen unsere tiefe Besorgnis über Artikel 7 des vorgeschlagenen Gesetzes über die Olympischen und die Paralympischen Spiele 2024 (projet de loi relatif aux jeux Olympiques et Paralympiques de 2024)[1] zum Ausdruck. Damit würde eine Rechtsgrundlage für den Einsatz von algorithmusgesteuerten Kameras zur Erkennung bestimmter verdächtiger Ereignisse im öffentlichen Raum geschaffen.

Der Vorschlag ebnet unter dem Vorwand, Großveranstaltungen zu sichern, den Weg für den Einsatz invasiver, algorithmengesteuerter Videoüberwachung. Mit dem Gesetz würde Frankreich der erste EU-Mitgliedsstaat, der solche Praktiken ausdrücklich legalisiert. Wir halten die vorgeschlagenen Überwachungsmaßnahmen für einen Verstoß gegen internationale Menschenrechtsvorschriften, da sie die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit verletzen und unannehmbare Risiken für Grundrechte wie das Recht auf Privatsphäre, die Versammlungs- und Vereinigungsfreiheit und das Recht auf Nichtdiskriminierung darstellen.

Wir fordern Sie auf den Artikel 7 zu hinterfragen und das Thema mit Organisationen der nationalen Zivilgesellschaft zu diskutieren. Dessen Verabschiedung würde einen besorgniserregenden Präzedenzfall für eine ungerechtfertigte und unverhältnismäßige Überwachung in öffentlich zugänglichen Räumen schaffen.

Der Vorschlag ist eine ernsthafte Bedrohung der bürgerlichen Freiheiten und der demokratischen Grundsätze.

Die bloße Existenz einer ungezielten (auch willkürlich zu bezeichnenden) automatisiert vorgehenden Videoüberwachung im öffentlich zugänglichen Raum kann eine abschreckende Wirkung auf die Inanspruchnahme bürgerlicher Grundfreiheiten haben, insbesondere auf das Recht auf Versammlungs-, Vereinigungs- und Meinungsfreiheit. Der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte[2] haben festgestellt, dass die biometrische Überwachung die begründete Erwartung der Menschen auf Anonymität im öffentlichen Raum untergräbt und aus Angst, identifiziert, profiliert oder sogar zu Unrecht verfolgt zu werden, ihre Fähigkeit und ihren Willen einschränkt ihre bürgerlichen Freiheiten auszuüben. Diese Maßnahme bedroht den Kern des Rechts auf Privatsphäre und auf Datenschutz und ist mit den internationalen und europäischen Menschenrechtsvorschriften nicht vereinbar.

Die Aufrechterhaltung des vollständigen Schutzes dieser Grundrechte und das Schaffen von Bedingungen, die eine öffentliche Debatte ermöglichen, einschließlich politischer Meinungsäußerung im öffentlichen Raum, ist bei wichtigen Ereignissen wie den Olympischen Spielen besonders bedeutend und steht in Einklang mit demokratischen Werten und Grundsätzen.

Die Gründe, die eine Überwachung des öffentlichen Raums rechtfertigen, werden durch das vorgeschlagene Gesetz erheblich und in gefährlicher Weise ausgeweitet. Die Einstufung von Betteln oder stationären Versammeln als „atypisch" birgt die Gefahr der Stigmatisierung und Diskriminierung von Menschen, die sich häufiger im öffentlichen Raum aufhalten, etwa wegen ihrer Obdachlosigkeit oder ihrer prekären wirtschaftlichen Situation.

Der Vorschlag würde zu einer biometrischen Massenüberwachung führen.

Artikel 7 Abs. 3 des Gesetzentwurfs behauptet fälschlich, dass algorithmische Videoüberwachungssysteme keine biometrischen Daten verarbeiten würden. Die europäische Datenschutz-Grundverordnung (DSGVO) definiert biometrische Daten als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen" (Art. 4 Nr. 14 DSGVO). Wenn der Zweck von algorithmusgesteuerten Kameras darin besteht bestimmte verdächtige Ereignisse in öffentlichen Räumen zu erkennen, erfassen und analysieren sie zwangsläufig physiologische Merkmale und Verhaltensweisen von Personen, die sich in diesen Räumen aufhalten, z.B. ihre Körperhaltung, ihren Gang, ihre Bewegungen, ihre Gesten oder ihr Aussehen. Ohne das Herausgreifen von Personen aus dem Gesamtbild wäre es unmöglich den Zweck des Systems zu erreichen, was auf eine „eindeutige Identifizierung" hinausläuft. Das europäische Datenschutzrecht legt gemäß der Auslegung durch den Europäischen Datenschutzausschuss[3] fest, dass die Fähigkeit, eine Person aus einer Menschenmenge oder ihrer Umgebung herauszuheben, eine „eindeutige Identifizierung" ist, unabhängig davon, ob der Name oder die ID-Nummer der Person bekannt ist.

Es muss darauf hingewiesen werden, dass der Einsatz von KI-basierten Systemen zur Analyse und Vorhersage des Verhaltens, der Emotionen oder der Absichten von Menschen ebenso invasiv und gefährlich sein kann wie der Einsatz von Systemen zur Identifizierung von Menschen. Die Einstufung von Personen als „risikoreich" auf der Grundlage ihrer biometrischen Daten käme

einer biometrischen Kategorisierung gleich, die vom französischen „défenseur des droits“ (Ombudsperson in Frankreich) und dem vorgeschlagenen EU-Gesetz über künstliche Intelligenz wegen ihrer biometrischen Merkmale als besondere Kategorie personenbezogener Daten definiert wird. Wir weisen Sie darauf hin, dass die Maßnahme im Widerspruch zu dem geplanten EU-Gesetz über künstliche Intelligenz stehen würde. Im Rahmen der aktuellen Gesetzgebung gibt es eine Reihe parlamentarischer Änderungsanträge, wonach die biometrische Kategorisierung wegen der damit verbundenen hohen Grundrechtsrisiken vollständig verboten werden soll.

Der schwerwiegende Eingriff in die Menschenrechte ist weder erforderlich noch verhältnismäßig.

Ein wirksamer Schutz der Menschenrechte setzt die Kenntnis der Grenzen der Technologien und den Nachweis voraus, dass sie das verfolgte Ziel wirksam erreichen. Daraus ergibt sich die Notwendigkeit zu untersuchen, wie die im Namen der Sicherheit eingeführten Technologien auf tatsächliche Bedrohungen reagieren und wie sie sich auf die Menschenrechte und bürgerlichen Freiheiten auswirken werden.

Der Gesetzesvorschlag stellt eine große Gefahr für grundlegende Menschenrechte dar und es gibt Hinweise dafür, dass Videoüberwachung bei der Verhinderung von Verbrechen oder Sicherheitsbedrohungen kein wirksames Mittel ist[4]. Demgemäß konnte die Regierung nicht dessen Erforderlichkeit und Verhältnismäßigkeit nachweisen; sie hat auch die Zivilgesellschaft in die Maßnahme nicht in sinnvoller Weise einbezogen. Darin liegt ein Verstoß gegen die staatliche Verpflichtung zur Wahrung der Menschenrechte gemäß internationalen Verträgen wie dem Internationalen Pakt über bürgerliche und politische Rechte und der Europäischen Menschenrechtskonvention.

Der Vorschlag ist ein Schritt auf dem Weg zur Gewöhnung an außergewöhnliche Überwachungsbefugnisse.

Der geplante Artikel 7 steht für den besorgniserregenden Trend von Regierungen ihre Überwachungsbefugnisse als Notmaßnahme im Namen der Sicherheit auszuweiten. Nur ausnahmsweise werden diese „außergewöhnlichen“ Maßnahmen zurückgenommen. Überwachung und Kontrolle werden vielmehr zur Normalität, zumeist ohne dass es angemessene Sicherheitsvorkehrungen, Transparenz, die Einbeziehung von Interessengruppen und Mechanismen zur Rechenschaftslegung gibt.

Dies gilt insbesondere für die Überwachungsmaßnahmen der letzten 20 Jahre im Namen der Terrorismusbekämpfung und – in jüngerer Zeit – für die digitalen Lösungen, die während der Covid-19-Pandemie eingeführt wurden[5]. Wir erlebten schon früher, dass Olympische Spiele entsprechend als Experimentierfeld zur Ausweitung staatlicher Befugnisse dienten, die später ohne Ausnahmeverhältnisse umgewidmet wurden[6].

Diese Erfahrungen begründen unsere Befürchtung, dass die algorithmische Videoüberwachung nach 2025 nicht abgeschafft würde. Die Verabschiedung dieses Gesetzes würde zudem einen gefährlichen Präzedenzfall für andere europäische Länder schaffen, die – bisher ohne Erfolg – riskante biometrische Überwachungspraktiken zu legalisieren versucht haben, so etwa Portugal und Serbien. Frankreich würde berüchtigter „Vorreiter“ der Überwachungspolitik in der Europäischen Union.

Wir hoffen aufrichtig, dass Sie im Austausch mit der Zivilgesellschaft die notwendigen Schritte vornehmen, um die in diesem Schreiben geäußerten Bedenken auszuräumen. Wir stehen für einen weiteren Austausch zu den angesprochenen Fragen zur Verfügung.

Mit freundlichen Grüßen

Access Now, Global; AlgoRace, Spain; AlgorithmWatch, Germany; AlgorithmWatch CH, Switzerland; Amnesty International, Global; ApTI, Romania; ARTICLE 19, Global; Association Nationale des Supporters, France; Big Brother Watch, UK; Bits of Freedom, The Netherlands; Centre for Democracy & Technology, Europe; Chaos Computer Club Lëtzebuerg, Luxembourg; Citizen D / Državljan D, Slovenia; Civil Liberties Union for Europe, Europe; **Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany;** Digitalcourage e.V., Germany; Digitale Gesellschaft, Switzerland; Digitale Freiheit e.V., Germany; Elektronisk Forpost Norge, Norway; Eticas Tech, Spain; European Center for Not-for-Profit Law Stichting (ECNL), Europe; European Digital Rights, Europe; Fair Trials, Global; Forum Civique Européen, France/Europe; Football Supporters Europe, Europe; Homo Digitalis, Greece; Human Rights Watch, International; Irish Council for Civil Liberties, Ireland; IT-Pol, Denmark; Iuridicum Remedium, Czech Republic; Liberty, UK; Panoptykon Foundation, Poland; Privacy International, Global; Privacy Network, Italy; Share Foundation, Serbia; Society Vrijbit, The Netherlands; Statewatch, Europe; Today is a new day / Danes je nov dan, Slovenia

1 https://www.senat.fr/leg/pjl22-220.html.

2 https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_fr.pdf.

3 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf.

4 https://ecnl.org/publications/under-surveillance-misuse-technologies-emergency-responses.

5 https://www.lemonde.fr/societe/article/2021/12/22/une-etude-commandee-par-les-gendarmes-montre-la-relative-inefficacite-de-la-videosurveillance_6106952_3224.html.

6 https://www.scielo.br/j/cm/a/zcKnN9ChT9Wqc4hfGWKSk4d/?format=pdf&lang=en.

Der englisch- und der französischsprachige Originalbrief ist im Internet abrufbar unter
https://edri.org/wp-content/uploads/2023/03/Civil-society-public-letter-on-Art.-7-of-the-French-Olympics-law-Final_EN.pdf
und
https://ecnl.org/news/civil-society-open-letter-proposed-french-law-2024-olympic-and-paralympic-games
(siehe hierzu die Meldung auf S. 107)

Europäisches Parlament: Stellen Sie sicher, dass das KI-Gesetz die Menschenrechte schützt!

Im Vorfeld der Abstimmung über das KI-Gesetz im Europäischen Parlament (AI-Act) fordert die Zivilgesellschaft die Mitglieder des Europäischen Parlaments (MdEP) auf dafür zu sorgen, dass das EU-Gesetz über künstliche Intelligenz (KI-Gesetz) den Grundrechten Vorrang einräumt und die von Systemen künstlicher Intelligenz (KI) betroffenen Menschen schützt.

In zunehmendem Maße werden KI-Systeme eingesetzt, um uns im öffentlichen Raum zu überwachen und zu identifizieren, unsere Kriminalitätswahrscheinlichkeit vorherzusagen, Polizei- und Einwanderungskontrollen auf bereits überwachte Gebiete vorzuverlagern, Verstöße gegen das Recht auf Asyl und die Unschuldsvermutung zu erleichtern, unsere Emotionen vorherzusagen und uns anhand diskriminierender Rückschlüsse zu kategorisieren sowie wichtige Entscheidungen über uns zu treffen, die unseren Zugang zu Sozialleistungen, Bildung und Beschäftigung bestimmen.

Ohne eine angemessene Regulierung werden KI-Systeme die bestehenden gesellschaftlichen Probleme der Massenüberwachung, der strukturellen Diskriminierung, der zentralisierten Macht großer Technologieunternehmen, nicht rechenschaftspflichtiger öffentlicher Entscheidungsfindung und der Umweltausbeutung weiter verschärfen. Die Komplexität, der Mangel an Rechenschaftspflicht und öffentlicher Transparenz sowie die wenigen verfügbaren Rechtsbehelfe stellen die Menschen vor die Herausforderung ihre Rechte durchzusetzen, wenn sie durch KI-Systeme geschädigt werden. Diese Hindernisse stellen vor allem für die am stärksten marginalisierten Mitglieder der Gesellschaft ein besonderes Risiko dar.

Der KI-Gesetzentwurf der EU kann und sollte diese Probleme angehen und sicherstellen, so dass die Entwicklung und Nutzung von KI innerhalb eines Rahmens von Rechenschaftspflicht, Transparenz und angemessenen, auf Grundrechten basierenden Einschränkungen erfolgt. Wir fordern die Abgeordneten des Europäischen Parlaments auf bei der Abstimmung über den KI-Gesetzentwurf Folgendes zu gewährleisten:

1. Befähigung der Menschen, die von KI-Systemen betroffen sind

- Gewährleisten Sie die horizontale und durchgängige Zugänglichkeit bei allen KI-Systemen.
- Stellen Sie sicher, dass Menschen, die von KI-Systemen betroffen sind, informiert werden und das Recht haben sich zu informieren, wenn sie von KI-gestützten Entscheidungen und Ergebnissen betroffen sind.
- Sehen Sie ein Recht für Betroffene vor sich bei einer nationalen Behörde zu beschweren, wenn ihre Rechte durch den Einsatz eines KI-Systems verletzt worden sind.
- Regeln Sie ein Recht auf Vertretung natürlicher Personen und ein Recht von Organisationen des öffentlichen Interesses eigenständige Beschwerden bei einer nationalen Aufsichtsbehörde einzureichen.
- Sehen Sie ein Recht auf wirksame Rechtsbehelfe bei Rechtsverletzungen vor.

2. Gewährleistung von Rechenschaftspflicht und Transparenz beim Einsatz von KI

- Regeln Sie die Verpflichtung für die Nutzer vor jedem Einsatz eines KI-Systems mit hohem Risiko eine Folgenabschätzung für die Grundrechte durchzuführen und zu veröffentlichen und die Zivilgesellschaft und die Betroffenen sinnvoll in diesen Prozess einzubeziehen.
- Alle Nutzer von KI-Systemen mit hohem Risiko und alle Nutzer von Systemen im öffentlichen Bereich sollten verpflichtet werden die Nutzung vor dem Einsatz in einer europäischen KI-Datenbank zu registrieren.
- Stellen Sie sicher, dass bei der Klassifizierung von KI-Systeme mit hohem Risiko der Rechtssicherheit Vorrang eingeräumt und den Anbietern keine Schlupflöcher eröffnet werden, um die rechtliche Prüfung zu umgehen.
- Stellen Sie sicher, dass in der EU ansässige KI-Anbieter, deren Systeme Auswirkungen auf Menschen außerhalb der EU haben, den gleichen Anforderungen unterliegen wie Anbieter innerhalb der EU.

3. Verbot von KI-Systemen, die ein unannehmbares Risiko für die Grundrechte darstellen

- Verbieten Sie vollständig und ausnahmslos die biometrische Identifizierung in Echtzeit und aus der Ferne in öffentlich zugänglichen Räumen durch alle Akteure.
- Verbieten Sie alle Formen von prädiktiven und profilbildenden Systemen in der Strafverfolgung und in der Strafjustiz (orts- und personengebunden).
- Verbieten Sie KI im Migrationskontext zur Erstellung individueller Risikobewertungen und -profile auf der Grundlage personenbezogener und sensibler Daten sowie von prädiktiven Analysesystemen, wenn diese zur Unterbindung, Einschränkung und Verhinderung von Migration eingesetzt werden.
- Verbieten Sie biometrische Kategorisierungssysteme, die natürliche Personen nach sensiblen oder geschützten Merkmalen kategorisieren, sowie die Verwendung jeglicher biometrischer Kategorisierungs- und automatisierter Verhaltenserkennungssysteme in öffentlich zugänglichen Räumen.
- Untersagen Sie den Einsatz von Emotionserkennungssystemen, die aus physischen, physiologischen, verhaltensbezogenen und biometrischen Daten auf die Emotionen und den Geisteszustand von Menschen schließen.

Wir fordern die Abgeordneten des Europäischen Parlaments auf für die Aufnahme dieser Schutzmaßnahmen in das Gesetz über künstliche Intelligenz zu stimmen und sicherzustellen, dass die Verordnung ein Instrument zur Förde-

rung der Grundrechte und der sozialen Gerechtigkeit ist.

Einen detaillierten Überblick darüber, wie das AI-Gesetz die Grundrechte besser schützen kann, finden Sie in dieser von 123 Organisationen der Zivilgesellschaft unterzeichneten Erklärung:
https://edri.org/our-work/civil-society-calls-on-the-eu-to-put-fundamental-rights-first-in-the-ai-act/

Weitere Informationen zu den von der Zivilgesellschaft vorgeschlagenen Änderungen finden Sie hier:
https://edri.org/our-work/the-eus-artificial-intelligence-act-civil-society-amendments/

Unterzeichnende 75 Organisationen: European Digital Rights (EDRi), Access Now, Algorithm Watch, Amnesty International, Article 19, Bits of Freedom, Electronic Frontier Norway (EFN), European Center for Not-for-Profit Law (ECNL), European Disability Forum, Fair Trials, Homo Digitalis, Irish Council for Civil Liberties (ICCL), Panoptykon Foundation, Platform for International Cooperation on the Rights of Undocumented Migrants (PICUM), #jesuisla, Afrique Culture Maroc, AI Forensics, AI Now Institute, Alternatif Bilisim (AiA), Alliance4Europe, Are You Syrious? Association for Juridical Studies on Immigration (ASGI), autonomic, Avaaz Foundation, Baobab Experience, Border Violence Monitoring Network, Centre for Youths Integrated Development, Civil Liberties Union for Europe, Coalition For Women In Journalism (CFWIJ), Coalizione Italiana Liberta e Diritti civili, Comision General Justicia y Paz, DataEthics.eu, Defend Democracy, **Deutsche Vereinigung für Datenschutz e.V. (DVD)**, Digitalcourage, Digitale Gesellschaft, Switzerland, Državljan D / Citizen D, Each One Teach One (EOTO) e. V., Ekō, Equipo Decenio Afrodescendiente Espana, Eumans, European Civic Forum, European Network Against Racism (ENAR), European Sex Workers Rights Alliance, Fair Trials, Fair Vote UK, Faith Matters EU, FUNDACION SECRETARIADO GITANO, Gong, Greek Forum of Migrants, Health Action International, Hermes Center, horizontl Collaborative, IT-Pol Denmark, Ivorian Community of Greece, La Strada International, Lafede.cat, Lie Detectors, Ligue des droits humains, Migrants' Rights Network, Mujeres Supervivientes, Open Knowledge Foundation Germany, ORBITvzw, Privacy International, Queerstion Media, Racism and Technology Center, Refugee Law Lab, York University, Refugees in danger (NGO) – Denmark, save space e.V., SOS RACISMO GIPUZKOA, Stichting The London Story, Superbloom (previously Simply Secure), The Daphne Caruana Galizia Foundation, UNI Europa, WeMove Europe

Entworfen von: European Digital Rights, Access Now, Algorithm Watch, Amnesty International, Article 19, Bits of Freedom, Electronic Frontier Norway (EFN), European Center for Not-for-Profit Law, (ECNL), European Disability Forum, Fair Trials, Homo Digitalis, Irish Council for Civil Liberties (ICCL), Panoptykon Foundation, Platform for International Cooperation on the Rights of Undocumented Migrants (PICUM).

Das englischsprachige Originaldokument ist im Internet zu finden unter
https://edri.org/wp-content/uploads/2023/04/PDF-FINAL-Statement-European-Parliament-Make-sure-the-AI-act-protects-peoples-rights.pdf.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

TK-Überwachung weiterhin auf hohem Niveau

Die Überwachung von Mobiltelefonnutzern mit verdeckten Mitteln durch Strafverfolgungsbehörden des Bundes bleibt auf hohem Niveau. Gemäß einer Antwort der Bundesregierung auf eine Anfrage der Linksfraktion im Bundestag führte die Bundespolizei im Jahr 2022 im Rahmen von strafprozessualen Ermittlungsverfahren in 105 Fällen Funkzellenabfragen durch. Bei dieser Methode werden die Verbindungsdaten aller zu einem bestimmten Zeitpunkt in einer Funkzelle eingebuchten Handy-Nutzer gespeichert und gerastert. 54 solcher Maßnahmen fanden im ersten, 51 im zweiten Halbjahr statt. 2021 waren es insgesamt 55 Fälle. Das Bundeskriminalamt (BKA) führte nur im ersten Halbjahr 2022 eine Funkzellenauswertung durch.

Das BKA verschickte 2022 in zahlreichen Ermittlungsverfahren und einem Gefahrenabwehrvorgang 51.950 „stille SMS", um Personen zu orten. 2021 waren es noch 68.152. Solche Kurzmitteilungen gehen an die anvisierten Mobiltelefone, werden dort aber nicht angezeigt. Das betroffene Gerät meldet sich bei der eingebuchten Funkzelle zurück, erzeugt so auswertbare Verbindungsdaten und verrät Ermittlern den ungefähren Standort der Nutzer, ohne dass diese das mitbekommen. Die Bundespolizei versandte 2022 in Eigenregie 19.703 dieser „Stealth Pings" in strafprozessualen Ermittlungsverfahren; zudem setzte sie 1360-mal auf externe Dienstleister. In einer gemeinsamen Ermittlungsgruppe mit der Landespolizei Baden-Württemberg kamen noch einmal 62 hinzu. Im Vergleich zu 2021 waren dies deutlich weniger. Die Beamten der Behörde griffen damals noch 47.951-mal zu diesem Instrument.

Beim Zoll behandelt das federführende Bundesinnenministerium (BMI) die einschlägige Statistik seit 2012 als Verschlusssache. Daran hat sich unter der Ampel-Koalition nichts geändert. Das BMI zeigte sich zwar erneut bereit eine „abstrahierte Aussage" zu stillen SMS beim Bundesamt für Verfassungsschutz zu übermitteln. Allerdings erfolgte diese nur eingestuft als Verschlusssache „für den Dienstgebrauch". Vor 2019 erreichte der Inlandsgeheimdienst Werte von bis zu 180.000 „Stealth Pings".

IMSI-Catcher brachte die Bundespolizei 2022 in 38 Fällen, das BKA „in je einem bereits abgeschlossenen Gefahrenabwehrvorgang und Ermittlungsverfahren" zum Einsatz, um den Standort eines aktiv geschalteten Mobiltelefons und die Geräte- oder Kartennummer zu ermitteln. Die Vergleichszahlen für 2021 lagen bei 44 beziehungsweise fünf Vorgängen. Die Generalbundesanwaltschaft ordnete ferner im vorigen Jahr in 42 Fällen den Einsatz eines IMSI-Catchers an. Zudem machte die Bundespolizei im ersten Halbjahr 2022 in einem Verfahren von einem „WLAN-Catcher" Gebrauch. Im zweiten Halbjahr sei das Werkzeug nicht genutzt worden. Im Widerspruch dazu spricht das BMI später aber von zwei Maßnahmen der Behörde, von denen insgesamt drei Personen betroffen gewesen seien.

Die Regierung teilte nur in eingestufter Form „für den Dienstgebrauch" mit, wie oft Bundesbehörden Staatstrojaner für die Quellen-Telekommunikationsüberwachung (TKÜ) oder heimliche Online-Durchsuchungen genutzt haben. Außen vor blieben auch die Geheimdienste, da eine Antwort dazu aus Sicherheitsgründen weiterhin nicht möglich sei. Bei der Soft- und Hardware für derlei Zwecke hätten sich gegenüber dem Vorjahr keine Änderungen ergeben. Bekannt ist, dass die Sicherheitsbehörden hier auf Eigenentwicklungen und kommerzielle Spyware wie Pegasus von der NSO Group setzen. Laut der aktuellen amtlichen Statistik für die Bundesländer und den Generalbundesanwalt gab es 2020 dort 25 Anordnungen zur Quellen-TKÜ (Krempl, Heimliche Überwachung: Deutlich mehr Funkzellenabfragen, weniger stille SMS, www.heise.de 07.04.2023, Kurzlink: https://heise.de/-8717037).

Bund

Extensive PNR-Erfassung wird eingeschränkt

Das Bundeskriminalamt (BKA) muss seine über Jahre hinweg praktizierte anlasslose und massenhafte Fluggastüberwachung aufgrund eines Urteils des Europäischen Gerichtshofs (EuGH v. 21.06.2022, DANA 3/2022, 201 ff.) sowie nationaler Rechtsprechung deutlich zurückfahren. Im Jahr 2022 konnte die Polizeibehörde bei der umstrittenen Himmels-Rasterfahndung aber noch einmal aus dem Vollen schöpfen: Luftfahrtunternehmen übermittelten in dem Jahr 424.305.929 sogenannte Passenger Name Records (PNR) an die beim BKA angesiedelte Fluggastdatenzentralstelle. Davon waren über 121 Millionen Flugpassagiere betroffen, wobei es zu Mehrfachnennungen aufgrund von Vielfliegern kommen konnte.

Die Zahlen stammen aus einer Antwort der Bundesregierung auf eine Anfrage der Linksfraktion des Bundestags. Die Zahlen liegen rund die Hälfte über denen von 2021, als die Airlines noch 211 Millionen Datensätze von etwa 62 Millionen Flugreisenden an die Sammelstelle geschickt hatten. 2020 waren es rund 100 Millionen PNR. Mit Stand vom 30.06.2022 waren so gemäß Regierungsmitteilung vom August 2022 rund 575 Millionen Datensätze im Fluggastdaten-Informationssystem gespeichert. Der Berg muss nun aber nach dem EuGH-Urteil schrumpfen, das die Hürden für die bisher praktizierte PNR-Vorratsspeicherung deutlich höher legte. Das Verwaltungsgericht Wiesbaden stufte

die BKA-Rasterfahndung daraufhin mit Urteil vom 06.12.2022 als rechtswidrig ein (DANA 1/2023, 65).

Um die PNR-Auswertung den EuGH-Anforderungen anzupassen, hat das Bundesinnenministerium (BMI) laut der Antwort „gemeinsam mit den betroffenen Behörden ein Maßnahmenpaket erarbeitet". Soweit die Luxemburger Richter „einen objektiven Zusammenhang zwischen strafbarer Handlung und der Beförderung von Fluggästen" forderten, werde dies inzwischen bei der Verarbeitung von Fluggastdaten geprüft. Die „Trefferausleitung" sei entsprechend eingeschränkt worden. Die Behörden arbeiteten zudem daran die EuGH-Ansage umzusetzen, dass PNR grundsätzlich nur noch sechs Monate gespeichert werden dürfen. Von April 2023 an greife eine entsprechende Löschkennzeichnung. Nur bei „verifizierten und ausgeleiteten Registertreffern" soll noch eine Aufbewahrung von bis zu fünf Jahren möglich sein.

PNR zu Flügen innerhalb der EU verarbeitet das BKA der Regierung zufolge nur noch, „wenn es hinreichend konkrete Umstände für die Annahme gibt", dass Deutschland „mit einer als real und aktuell oder vorhersehbar einzustufenden terroristischen Bedrohung konfrontiert ist". Das BMI erarbeite zudem einen Referentenentwurf für eine Novelle des Fluggastdatengesetzes und werde diesen dann im Ressortkreis abstimmen. Einen konkreten Zeitplan dafür gebe es noch nicht. Den Entwurf der EU-Kommission, parallel mehr API-Daten (Advance Passenger Information) zu sammeln und über einen zentralen Router an zuständige Behörden zu übermitteln, müsse man noch genauer bewerten.

Die Zahl der „fachlich positiv überprüften und deshalb ausgeleiteten Vorgänge" auf Basis des Abgleichs der PNR mit anderen Datenbanken zur Personen- und Dokumentenfahndung sowie einer vom BKA durchgeführten Mustererkennung war auch 2022 mit 87.845 überschaubar. 19.827 verdächtige Passagiere traf die Polizei vor Ort an, 1.387 nahm sie fest, während es 2021 1.052 waren. Dies verursachte beträchtliche Ausgaben: Bis zur Inbetriebnahme der Fluggastdatenzentralstelle im August 2018 sind im BKA für deren Aufbau Kosten von 13,75 Millionen Euro entstanden, dem Bundesverwaltungsamt (BVA) für den Aufbau des zugehörigen Informationssystems 40,55 Millionen Euro. Die laufenden Betriebskosten lagen allein 2022 bei 3,2 beziehungsweise 11,4 Millionen Euro – der Einsatz internen Personals nicht eingerechnet.

Die Linken-Innenpolitikerin Martina Renner kritisierte: „Das PNR-System schluckt weiterhin die Daten von Millionen unbescholtener Bürgerinnen und Bürger." Erste Ansätze zur Einschränkung und Löschung nach sechs Monaten seien zwar Fortschritte, „aber das Grundproblem besteht fort". Letztlich werde nur ein Bruchteil der Daten überhaupt genutzt und nur ein Fünftel der gesuchten Personen tatsächlich an den Flughäfen von der Polizei angetroffen. Die Bundesregierung habe ihre eigenen Vorhaben im Koalitionsvertrag offenbar bereits vergessen: „Chatkontrolle, Vorratsdaten oder PNR zeigen, wie ernst sie den Schutz der Bürger und ihrer Daten tatsächlich nimmt." Die Linksfraktion hält die PNR-Speicherung generell für „in hohem Maße unverhältnismäßig" und zu personalintensiv angesichts hunderter Planstellen beim BVA und BKA (Krempl, Himmels-Rasterfahndung: BKA erhielt 424 Millionen neue Fluggastdaten in 2022, www.heise.de 02.05.2023, Kurzlink: https://heise.de/-8985231)

Bund

CDU kritisiert Faesers Social-Media-Account-Wechsel

Die CDU hat den Bundesbeauftragten für den Datenschutz (BfDI), Ulrich Kelber, aufgefordert die Social-Media-Konten der hessischen SPD-Spitzenkandidatin Nancy Faeser zu überprüfen. Faesers Konten waren bis Februar 2023 vom Bundesinnenministerium betreut worden. CDU-Innenpolitiker Philipp Amthor kritisierte, dass diese Konten mit der amtlichen Kommunikation „ungefiltert an die SPD Hessen übertragen" worden sei. Wäre dies eine rechtskonforme Übertragung, hätte auch Angela Merkel nach Amtsende ihre Konten auf die CDU umschreiben können: „Dagegen würde jedes Rechtsempfinden sprechen". Amthor spricht vom „Trick einer fingierten Einwilligung". Es sei nicht im Sinne des Schutzes von Kommunikationsdaten, dass amtliche Informationen einseitig an eine Partei im Wahlwettbewerb übertragen werden können. Faeser hatte im Februar angekündigt am 08.10.2023 für die SPD bei der hessischen Landtagswahl zu kandidieren. Die Sozialdemokratin will nur im Falle eines Sieges nach Hessen gehen (Der Spiegel Nr. 18 29.04.2023, 9).

Bund

Erster BND-Kontrollratsbericht

Der Anfang 2022 eingerichtete Unabhängige Kontrollrat (UKR) für den Bundesnachrichtendienst (BND), der Anordnungen der Spitze des Auslandsgeheimdienstes für Maßnahmen zur Überwachung vorab prüfen muss, hat gemäß Medienberichten einen ersten schriftlichen 60-seitigen Bericht an das Parlamentarische Kontrollgremium (PKGr) des Bundestags übermittelt. Demnach soll das vor allem mit Richtern des Bundesgerichtshofs beziehungsweise des Bundesverwaltungsgerichts besetzte Gremium bislang nur einen von 121 Überwachungsanträgen beanstandet und so fast alle Ersuchen genehmigt haben.

Der Bundestag hatte 2021 eine Reform des BND-Gesetzes beschlossen, mit welcher der Auslandsgeheimdienst eine breite Befugnis zum Hacken ausländischer Vermittlungsanlagen, Telekommunikationsinfrastruktur und IT-Systeme von Providern erhielt. Der BND darf demnach auch offiziell in Computer und Handys von Ausländern im Ausland mit technischen Mitteln wie dem Bundestrojaner eindringen und heimliche Online-Durchsuchungen durchführen. Zu den vom UKR begutachteten Fällen gehören auch Hacking-Operationen, bei denen die Agenten in Chats über Messenger und andere Online-Kommunikation eindringen. Eingeschlossen waren gemäß dem Bericht ferner Anträge zum klassischen Abhören von Telefonaten und Funksprüchen oder zum Mitlesen von E-Mails.

54% der BND-Maßnahmen aus dem vergangenen Jahr sollen die seit Jah-

ren umstrittene verdachtsunabhängige Massenüberwachung in Form der strategischen Fernmeldeaufklärung betreffen. Das Bundesverfassungsgericht hatte den dafür von dem Geheimdienst verwendeten Datenstaubsauger für verfassungswidrig erklärt (DANA 3/2020, 202 ff.). Der Bundestag hielt das Instrument aber grundsätzlich für unverzichtbar. Nach wie vor darf der BND so abgezogene Netzkommunikation anhand von Selektoren durchsuchen, obwohl die Ergebnisse trotz tausender eingesetzter Suchbegriffe wenig ergiebig zu sein scheinen.

Der UKR kann in Folge des Karlsruher Urteils die ausgewählten Selektoren einsehen, um einen zweiten GAU wie nach dem ungeprüften Einsatz von NSA-Suchbegriffen zu verhindern. Der BND habe sich hier jederzeit kooperativ gezeigt, so der Bericht. Der Geheimdienst habe umfangreich Zugang gewährt, und zwar zu Unterlagen, Daten und Technik. Auch die Selektoren ausländischer Partnerdienste, mit denen der BND die weltweite Kommunikation durchsucht, konnten die Prüfer offenbar einsehen. Insbesondere bei der Abteilung für die Technische Aufklärung, die in Pullach verblieben ist, sei der Frust über die zusätzliche Mehrarbeit bei der Beantragung von Überwachungsaktionen mit teils seitenlangen Begründungen aber groß.

40% der Spähersuchen sollen Einzelpersonen betroffen haben, die gezielt überwacht wurden. Die übrigen 60% seien „qualifizierte Aufklärungsmaßnahmen" gewesen, also besonders aufwändige Operationen etwa mithilfe von Staatstrojanern auf Computern oder Mobiltelefonen. Die einzige Beanstandung habe sich auf eine Überwachungsanordnung für eine „juristische Person" in Deutschland bezogen, also eine Firma, deren Verbindungen ins Ausland ausspioniert werden sollten. Dies sei nach Ansicht des Rats nicht vom BND-Gesetz gedeckt gewesen. Es hätten für die beantragte Spähaktion einzelne Zielpersonen benannt werden müssen (Krempl, Bundesnachrichtendienst: Kontrollrat winkt fast alle Überwachungsersuchen durch, www.heise.de 21.04.2023; Kurzlink: https://heise.de/-8975862).

Bund

Novellierung des Bundespolizeigesetzes

Die Fraktionen der Regierungskoalition aus SPD, Grünen und FDP haben sich nach langen Auseinandersetzungen darauf geeinigt, dass die Bundespolizei keinen Staatstrojaner einsetzen darf. Im Gegensatz zur vorherigen schwarz-roten Koalition soll die Bundespolizei keine staatliche Malware direkt auf dem Endgerät eines Verdächtigen installieren dürfen, um Daten vor einer Verschlüsselung oder nach einer Entschlüsselung zu kopieren (Telekommunikationsüberwachung an der Quelle, Quellen-TKÜ).

Der Koalitionsvertrag stellt klar: „Das Bundespolizeigesetz novellieren wir ohne die Befugnis zur Quellen-TKÜ und Online-Durchsuchung". Trotzdem drängte das Bundesinnenministerium darauf. Der Bundestag hatte Juni 2021 bereits einen Entwurf zur Novelle des Bundespolizeigesetzes beschlossen, der eine Erlaubnis zum Einsatz von Staatstrojanern enthielt. Die Bundespolizei sollte so an Kommunikation herankommen, die über verschlüsselte Dienste wie WhatsApp, Signal oder Threema läuft. Der Bundesrat stimmte der Initiative aber wegen damit verknüpfter weiter Einschnitte in die Kompetenzen der Länderpolizeien nicht zu. Der frühere Bundesinnenminister Horst Seehofer (CSU) wollte neben der Lizenz für die heimliche Online-Durchsuchung und die Quellen-TKÜ auch die biometrische Gesichtserkennung zulassen. Die SPD hatte bei letzterer aber Bedenken, sodass der Kompromiss auf die Quellen-TKÜ hinauslief. Dagegen legten nun Grüne und FDP unter Verweis auf den Koalitionsvertrag ihr Veto ein.

Neu gefasst werden sollen mit dem jetzigen Anlauf die Vorschriften zum Erheben und Auswerten von Bestands-, Nutzungs- und Verkehrsdaten. Bund und Länder hatten sich schon im März 2021 im Vermittlungsausschuss auf Korrekturen an einem umstrittenen Gesetzentwurf verständigt, mit dem die Regeln für die Bestandsdatenauskunft an die Vorgaben des Bundesverfassungsgerichts von 2020 angepasst werden sollen. Damit darf neben dem Bundeskriminalamt auch die Bundespolizei im Kampf gegen schwere Straftaten Passwörter bei Telemediendiensten wie WhatsApp, eBay, Facebook, Gmail, YouTube oder Tinder abfragen.

Die Innenpolitiker des Regierungsbündnisses vereinbarten zudem eine Klausel gegen Racial Profiling. Diese soll Polizeikräften eine rechtssichere Grundlage für Kontrollen geben, ohne dass dabei der Verdacht entsteht, sie würden ausschließlich aufgrund äußerer Merkmale durchgeführt. Ein entsprechendes Erscheinungsbild soll einer Überprüfung aber nicht im Wege stehen, wenn Erfahrung oder aktuelle Ereignisse sie angemessen erscheinen lassen. Im Gegenzug können überprüfte Personen eine Kontrollquittung erhalten, wenn sie das verlangen. Damit soll der Verlauf einer Personenprüfung dokumentiert werden ohne Polizeiarbeit unter Generalverdacht zu stellen.

Die EU-Kommission hat 2022 ein Vertragsverletzungsverfahren gegen Deutschland eingeleitet, weil es die EU-Richtlinie zum Datenschutz bei Polizei und Justiz von 2016 nicht komplett umgesetzt hat. Grund dafür sind fehlende Vorgaben für die Bundespolizei. Der Bundesdatenschutzbeauftragte Ulrich Kelber kann dort Datenschutzverstöße bisher nur beanstanden; ihm fehlen wirksame Durchsetzungsbefugnisse. SPD-Innenexperte Sebastian Hartmann erläuterte, dass sich die Regierungsressorts bei der überfälligen Reform verhakt hätten. Jetzt hätten die Fraktionen selbst eine Lösung gefunden. Seitens der Grünen ist von einer „Richtungsentscheidung für die Modernisierung der Bundespolizei" die Rede, seitens der FDP von einer Einigung, die Freiheit und Sicherheit der Bürger gleichermaßen stärke (Krempl, Kein Staatstrojaner für deutsche Bundespolizei, www.heise.de 25.04.2023, Kurzlink: https://heise.de/-8978967).

Bundesweit

Datenschutzaufsicht stellt Fragen an OpenAI wegen ChatGPT

Ende April 2023 wurde OpenAI, der Anbieter von ChatGPT, von den deut-

schen Datenschutzaufsichtsbehörden der Länder, die für privatwirtschaftliche Unternehmen zuständig sind, zur Beantwortung eines Fragenkatalogs zur Datenschutzkonformität der Anwendung aufgefordert. Die Aufsichtsbehörden haben sich auf ein gemeinsames Musterschreiben geeinigt und ein Verwaltungsverfahren gegen den in San Francisco ansässigen Konzern eröffnet.

Die Fragen an OpenAI betreffen laut dem hessischen Datenschutzbeauftragten Alexander Roßnagel die Gewährleistung des Grundrechts- und Datenschutzes bei der Nutzung dieses Dienstes: „Je nach Fragen- oder Aufgabenstellung an ChatGPT gibt die nutzende Person unterschiedlich viele, teils sensitive Informationen von sich preis – etwa zu Interessen an politischen, religiösen, weltanschaulichen oder wissenschaftlichen Fragen oder zu ihrer familiären oder sexuellen Lebenssituation. Auch können Fragen über andere Personen gestellt werden. Unklar ist, zu welchen Zwecken eingegebene Daten verarbeitet werden und aus welchem Datenpool die hinter dem Dienst liegende, künstliche Intelligenz ihr Wissen speist. Erst wenn diese Fragen beantwortet wurden, kann ich prüfen, ob sich OpenAI mit ChatGPT an die europäischen Datenschutzvorgaben hält."

Wichtig sei, ob die Datenverarbeitung den datenschutzrechtlichen Grundprinzipien gerecht werde, ob sie auf einer gültigen Rechtsgrundlage beruhe und ob sie für die Betroffenen ausreichend transparent sei. Zum Schutz von Kindern und Jugendlichen werde gefragt, welche Altersgrenze für die Nutzung von ChatGPT bestimmt ist, wie die Einhaltung der Altersgrenze überprüft wird und ob für alle Nutzenden unter 16 Jahren die Einwilligung der Erziehungsberechtigten eingeholt wird. Zudem wolle man von OpenAI erfahren, ob die Nutzungsdaten als Trainingsdaten im Rahmen des maschinellen Lernens verwendet werden, welche Quellen für die Auskünfte über Personen genutzt werden und für welche Zwecke – wie etwa Profilbildung und Werbung – die Nutzungsdaten gespeichert werden.

Die Datenschutzkonferenz (DSK) des Bundes und der Länder befasst ihre KI-Taskforce mit dem Thema ChatGPT; die Taskforce soll dabei das Vorgehen der Aufsichtsbehörden koordinieren. Da OpenAI keine Niederlassung in der EU hat, sind die jeweiligen Datenschutzaufsichtsbehörden der Mitgliedsstaaten dafür zuständig in ihrem Zuständigkeitsbereich die Einhaltung der Datenschutz-Grundverordnung (DSGVO) durch den Konzern zu überwachen. In Italien sprach die Datenschutzbehörde Ende März ein vorläufiges Verbot aus (s.u. S. 107).

Dieter Kugelmann, Leiter der Bundesländer-Taskforce für „Künstliche Intelligenz" (KI), erklärte: „Wenn personenbezogene Daten verwendet werden, auch als Trainingsdaten für die KI, dann bedarf es einer Rechtsgrundlage. Wir müssen wissen, wo die Daten herkommen." Ohne Rechtsgrundlage wäre der Betrieb von ChatGPT illegal. Kugelmann ist seit 2015 Landesbeauftragter für Datenschutz und Informationsfreiheit in Rheinland-Pfalz. Er hält das Vorgehen der Italiener für „riskant und rein rechtlich auf wackeligen Beinen". Zuerst müsse die Funktionsweise von ChatGPT geklärt sein. „Das breitflächige Ausrollen der KI im Blindflug – ohne rechtliche Grundlage – das ist das Hauptproblem."

Roßnagel ergänzte: „Sobald uns die Antwort von OpenAI vorliegt, werde ich mich mit den anderen Aufsichtsbehörden in Deutschland und Europa in der Bewertung der Antworten abstimmen. Als Reaktion auf die Bewertung kann ich nach der DSGVO vielfältige und wirksame Instrumente nutzen. Dabei geht es mir nicht darum der gesellschaftlichen Bewertung von KI-Systemen vorzugreifen. Vielmehr fordere ich von amerikanischen KI-Anbietern den gleichen Datenschutz wie von europäischen Anbietern."

Die Datenschutzbeauftragte Schleswig-Holsteins und Vorsitzende der Datenschutzkonferenz (DSK), Marit Hansen, bestätigte, dass die Datenschutzbeauftragten der Länder „standardisierte Fragen" an ChatGPT-Entwickler OpenAI versenden. Sie rechnet damit, dass die Beantwortung durch OpenAI „noch lange dauern" könnte. Über eine tatsächliche Sperre könne man erst im „übernächsten Schritt" – nach Auswertung und Prüfung der erhaltenen Auskünfte – nachdenken. Zudem seien die konkreten Zuständigkeiten dafür in Deutschland nicht eindeutig.

OpenAI wurde 2015 gegründet, unter anderen von Peter Thiel, Elon Musk und Amazon. Ursprünglich war es ein gemeinnütziges Forschungsprojekt, dessen Erkenntnisse frei zugänglich waren. Seit 2019 ist hingegen die gewinnorientierte Tochterfirma OpenAI LP der operative Arm. Damals hatte sich Microsoft mit einer Milliarde US-Dollar in OpenAI eingekauft.

Am 20.04.2023 hat Twitter-Chef Elon Musk angekündigt Microsoft zu verklagen, weil ChatGPT ohne entsprechende Lizenz auch anhand von Twitter-Daten trainiert worden sei. Der plötzliche Unmut dürfte daher rühren, dass Microsofts Reklameplattform ab 25.04.2023 keine Verwaltung von Twitter-Konten mehr unterstützt. Hintergrund für diesen Schritt sind die hohen Gebühren, die Musk für den Zugriff auf Twitters Schnittstellen eingeführt hat (Müller, Hessischer Datenschützer fordert Antworten zu ChatGPT, Tagesspiegel Background Digitalisierung & KI, 21.04.2023; Sokolov, ChatGPT: Deutschlands Datenschützer eröffnen Verfahren gegen OpenAI, www.heise.de 20.04.2023, Kurzlink: https://heise.de/-8974708).

Bundesweit

DSK beschließt eigene Geschäftsstelle

Auf der Zwischenkonferenz der Datenschutzkonferenz (DSK) vom 22.03.2023 hat sich diese für die Einrichtung einer DSK-Geschäftsstelle ausgesprochen. Gemäß Marit Hansen, Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), die 2023 den Vorsitz der DSK innehat, soll die neue Einrichtung helfen die Kooperation und Koordination der Datenschutzaufsichtsbehörden zu verbessern und zu effektivieren. Die Geschäftsstelle soll von Bund und Ländern gemeinsam errichtet und unterhalten werden. Der Arbeitskreis DSK 2.0 hat seit einiger Zeit insofern Vorschläge entwickelt. Auf der vorangegangenen Datenschutzkonferenz 2022 war die Errichtung eines Präsidiums der DSK beschlossen worden, das 2023 als Pilotprojekt eingesetzt werden soll. Dieses soll aus fünf Mitglie-

dern, dem vorherigen, aktuellen und nächstjährigen Vorsitz sowie den beiden Vertretern im Europäischen Datenschutzausschuss (EDSA) bestehen (Datenschutzkonferenz richtet Geschäftsstelle ein, Tagesspiegel, Digitalisierung & KI, 23.03.2023).

Bundesweit

noyb geht gegen Facebook-Werbung politischer Parteien vor

Der Datenschutzverein noyb (none of you business) hat am 21.03.2023 bei deutschen Datenschutzbehörden Beschwerden gegen AfD, CDU, Grüne, die Linke, ÖDP und SPD wegen ihrer Facebook-Werbung eingereicht, bei der die politischen Ansichten der Nutzer ausgewertet wurden. Er wirft den Parteien vor während der Bundestagswahl 2021 mithilfe von Microtargeting auf Facebook potenziellen Wählern personalisierte Anzeigen mit Wahlversprechen vorgesetzt zu haben. Diese gezielte Ansprache sei mit der Datenschutz-Grundverordnung (DSGVO) unvereinbar, da durch sie politische Meinungen besonders geschützt würden. Das Vorgehen sei rechtswidrig und berge „erhebliche Gefahren für die Demokratie“ und die Privatsphäre der Betroffenen.

Die TV-Sendung „ZDF Magazin Royale“ hatte zwei Tage vor der Bundestagswahl den Microtargeting-Einsatz bei politischer Facebook-Reklame aufgedeckt. Nach der Sendung hatten zahlreiche Facebook-Nutzer eingewilligt noyb ihre Daten zu übergeben und dafür eine Browsererweiterung installiert (DANA 4/2021, 247 f.). Damit konnte der Verein eigenen Angaben zufolge konkrete DSGVO-Verstöße ausfindig machen. Die Auswertung ergab, dass viele deutsche Parteien Facebook-Nutzer mit politischer Werbung adressierten, die auf deren Interessen zugeschnitten war. Dies sei zwar nicht verboten, betont noyb, doch konnten die Parteien die Nutzer nur auswählen, „weil Facebook im Hintergrund deren politische Ansichten ausgewertet hatte“. Der Verein sieht darin einen DSGVO-Verstoß sowohl der Parteien als auch des Plattformbetreibers.

Felix Mikolasch, Datenschutzjurist bei noyb, erläuterte dazu, dass Daten zur politischen Einstellung von Personen nicht nur extrem sensibel seien. Sie erlaubten auch „großflächige Manipulation von Wählern“. Dies habe der Fall Cambridge Analytica gezeigt. Die Beschwerden des Vereins sind fast alle an die Berliner Datenschutzbeauftragte Meike Kamp gerichtet, weil die Parteien ihren Sitz in der Hauptstadt haben. Die Eingabe wegen der ÖDP ging an das für die Ökopartei zuständige Bayerische Landesamt für Datenschutzaufsicht. Von den im Bundestag sitzenden Parteien blieben die CSU und die FDP außen vor (Krempl, Microtargeting: Datenschutz-Lobby beschwert sich über deutsche Parteien, www.heise.de 21.03.2023, Kurzlink: https://heise.de/-7601521).

Bundesweit

Schufa verkürzt Privatinsolvenzdaten-Speicherfrist von 3 Jahren auf 6 Monate

Vor dem Hintergrund laufender Gerichtsverfahren verkürzt die Schufa ab sofort die Speicherdauer für die Einträge zu abgeschlossenen Privatinsolvenzen von drei Jahren auf sechs Monate. Schufa-Vorstand Ole Schröder teilte am 28.03.2023 mit, damit wolle man Klarheit und Sicherheit für die Verbraucherinnen und Verbraucher schaffen: „Wir ermöglichen so den Restschuldbefreiten einen schnellen wirtschaftlichen Neustart.“ Am Morgen dieses Tages hatte der Bundesgerichtshof (BGH) bekannt gegeben, dass er ein Verfahren zu der bisher umstrittenen Frage der zulässigen Speicherdauer vorerst aussetzt. Er will eine Entscheidung des Europäischen Gerichtshofs (EuGH) in zwei ähnlichen Fällen abwarten.

Durch eine Verbraucherinsolvenz können sich Privatpersonen von ihren Schulden befreien, auch wenn sie nicht alles zurückzahlen können. Am Ende steht die sogenannte Restschuldbefreiung. Die Information darüber wird sechs Monate lang auf einem amtlichen Internetportal veröffentlicht. Die Schufa und andere Auskunfteien erheben diese Bekanntmachungen und speichern sie drei Jahre lang. Mitte März 2023 hatte sich der zuständige EuGH-Generalanwalt sehr kritisch zu der langen Speicherung geäußert. Für Betroffene habe das erhebliche negative Folgen. Die EuGH-Richter sind an die Einschätzung des Generalanwalts nicht gebunden, folgen ihr aber oft.

Die Insolvenzangaben fließen in den Schufa-Score ein. Dessen Rechtmäßigkeit wird ebenfalls angezweifelt. Die Berechnungsmethode hierfür wird als Geschäftsgeheimnis behandelt, was der Bundesgerichtshof (BGH) vor Jahren akzeptierte. Das Verwaltungsgericht Wiesbaden legte den Fall dem EuGH vor, um grundsätzlich das Verhältnis zur europäischen Datenschutz-Grundverordnung (DSGVO) klären zu lassen. Die DSGVO schreibt in Art. 22 vor, dass Entscheidungen, die für Betroffene rechtliche Wirkung entfalten, nicht nur durch die automatisierte Verarbeitung von Daten getroffen werden dürfen. Die Kreditwirtschaft und der Online-Handel nutzen den Score als Grundlage für Entscheidungen über die Behandlung von Kunden. Der Generalanwalt befand, dass bereits die automatisierte Erstellung eines Wahrscheinlichkeitswerts über die Kreditwürdigkeit – des Score-Werts – eine solche verbotene automatische Entscheidung darstellt (Tobias Költzsch/dpa, Schufa speichert Privatinsolvenzen nur noch 6 Monate lang, www.golem.de 28.03.2023; Janisch/Wischmeyer, Schufa knickt ein, SZ 29.03.2023, 16).

Baden-Württemberg

Keber folgt Brink

Nach dem Weggang von Stefan Brink Ende 2022 war die Stelle des Landesbeauftragten für Datenschutz in Baden-Württemberg unbesetzt. Die Landesregierung hat den Professor der Hochschule der Medien in Stuttgart, den 49-jährigen Wissenschaftler und Juristen Tobias Keber, benannt. Er ist seit über zehn Jahren in Stuttgart Lehrbeauftragter für Medienrecht und Medienpolitik in der digitalen Gesellschaft sowie Lehrbeauftragter für Internetrecht im Masterstudiengang Medienrecht am Medieninstitut an der Johannes Gutenberg-Universität Mainz. Er

ist Vorsitzender des Wissenschaftlichen Beirats der Gesellschaft für Datenschutz und Datensicherheit (GDD), im Herausgeberbeirat der Fachzeitschrift Recht der Datenverarbeitung (RDV) sowie im Leitungsgremium des Instituts für Digitale Ethik (IDE) an der Hochschule der Medien Stuttgart. Keber war vor seiner akademischen Laufbahn als praktizierender Rechtsanwalt tätig und ist Autor von Fachpublikationen zum nationalen und internationalen Medien-, IT- und Datenschutzrecht.

Die Grünen hatten bei der Personalie das Vorschlagsrecht. Keber muss vom Landtag bestätigt werden. Sein Vorgänger, das FDP-Mitglied Brink, hatte sein Amt nach einer Amtsperiode von sechs Jahren niedergelegt. Brink galt als unbequemer Kritiker der Landespolitik. Vor allem den baden-württembergischen Innenminister Thomas Strobl (CDU) hatte er in Bedrängnis gebracht. In einem Gutachten zur sogenannten Polizeiaffäre hatte Brink dem Minister vorgeworfen mit der Weitergabe eines Anwaltsschreibens gegen den Datenschutz verstoßen zu haben. Keber hat nun über das offizielle Datenschutzverfahren gegen Strobl zu entscheiden (Stuttgarter Medienrechts-Professor wird oberster Datenschützer in BW, www.swr.de 28.03.2023).

Bayern

Datenschutzkontrolle nach Datenleck bei „Letzter Generation“

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat ein Prüfverfahren gegen die „Letzte Generation“ nach Berichten über ein Datenleck bei der Klimaschutzbewegung eingeleitet. Diese sammelte demnach persönliche Daten von über 2.200 Anhängern und Interessenten mit teils hochsensiblen politischen Einschätzungen auf einer Excel-Liste, die sie frei zugänglich auf den Cloud-Dienst Google Drive einstellte. Darauf verzeichnet waren Anmerkungen wie: „Zu ängstlich für Gefängnis.“

Die Kontrolleure wollen klären, ob die Daten wirklich für jedermann einsehbar oder Zusatzkenntnisse wie „ein spezifischer Zugangslink erforderlich“ waren. Eine BayLDA-Sprecherin meinte, im zweiten Fall wäre dann die Ausgestaltung der Weitergabe der URL zu bewerten: „Letztendlich bewerten wir bei einem solchen Vorfall das Risiko für die betroffenen Personen.“ Sei dieses hoch, müssten sie über den Vorfall unterrichtet werden. „Zusätzlich legen wir bei der Aufarbeitung von Sicherheitsverletzungen grundsätzlich großen Wert darauf, dass sich diese nicht ohne Weiteres nochmals ereignen können.“ Dabei gehe es etwa um die zusätzliche Absicherung einer Datei in der Cloud mit einem „starken Passwort“. Generell sei das BayLDA für die Webseite https://letztegeneration.de/ zuständig. Ob das auch so bei der Frage der sonstigen Verarbeitung personenbezogener Daten bleibe, werde sich erst im Laufe des Verfahrens herausstellen. Im Impressum des Webauftritts der Gruppe ist ein Techniker mit Wohnsitz in Augsburg als Verantwortlicher eingetragen.

Der Berliner Rechtsanwalt Niko Härting bewertet die Panne als „Daten-Super-GAU“. Die besonders schützenswerten persönlichen Informationen dürften auch nicht auf einem Google-Drive-Konto gespeichert werden, das mit restriktiven Zugriffsrechten besser abgeschirmt ist. Er bemängelte in diesem Sinne auch die Datenschutzerklärung auf der Webseite der Klima-Aktivisten: „Da es die Excel-Liste gibt, wissen wir, dass man Profile zu einzelnen Personen erstellt.“ In der Erklärung finde sich aber nur der Hinweis: „Deine Daten werden zum einen dadurch erhoben, dass du uns diese mitteilst.“ Über eine Profilbildung informiere die Gruppe also nicht, genauso wenig über deren Zwecke und wer die Zusammenstellung erhalten und nutzen könne.

Laut der BayLDA-Sprecherin gab es bislang für die Behörde „keinen Anlass die Datenschutzerklärung zu prüfen“. Aufgrund der Vielzahl von Webseiten gebe es keine anlasslosen Kontrollen. Sollte dazu aber etwa eine Datenschutzbeschwerde eingehen oder andere Faktoren vorhanden sein, die ein höheres Risiko in diesem Zusammenhang ergeben, „dann wird diese Prüfung entsprechend der angezeigten Priorisierung unserer Aufgaben durchgeführt“. Zum Fall der Letzten Generation hätten das Amt noch keine Eingaben Betroffener erreicht.

Gemäß Art. 33 DSGVO müssen Verantwortliche bei einem Verstoß diesen nach Bekanntwerden „unverzüglich und möglichst binnen 72 Stunden“ melden. Ob die Letzte Generation sich fristgerecht an die Behörde wendete, ist offen. Das BayLDA erteilt dazu nach eigenen Angaben grundsätzlich keine Auskunft. Die Letzte Generation äußerte sich auf Anfrage nicht zu dem Thema und zu möglicherweise inzwischen ergriffenen Vorsichtsmaßnahmen. Ein Sprecher bat um einen weiteren „Moment Geduld“.

Politiker äußerten sich kritisch, so z.B. Konstantin von Notz, Vize der Grünen-Bundestagsfraktion: „Wer Menschen anleiten und vernetzen will, dem kommt eine besondere Verantwortung beim Schutz ihrer persönlichen Daten zu.“ Die Zuständigen der Letzten Generation seien dem absolut nicht gerecht geworden. Auch an ersten beschwichtigenden, den gravierenden Vorfall herunterspielenden Statements werde deutlich: Offenkundig hätten sich die Verantwortlichen „bislang viel zu wenig mit grundlegenden Fragen von Grundrechtsschutz und IT-Sicherheit beschäftigt“. Nachhaltigkeit im Digitalen bedeute aber auch „sichere und datenschutzkonforme Systeme zu nutzen“. Manuel Höferlin, innenpolitischer Sprecher der FDP-Bundestagsfraktion, kündigte eine schärfere Beobachtung der Organisation an: „Wer die Bereitschaft seiner Mitglieder erfasst, ins Gefängnis zu gehen, und sie für Blockadeaktionen schult, der hat offensichtlich strafrechtlich relevante Absichten. Da sich die Letzte Generation immer weiter radikalisiert, ist es richtig, dass wir ihre Blockadeaktionen zukünftig in einem bundesweiten Lagebild erfassen.“ Das Leck zeige aber auch, wie wichtig digitale Bildung sei: „Angehende Klimachaoten sollten neben dem How-to-Festnahme-Seminar vielleicht auch einen Crashkurs in Datenschutz absolvieren.“

Die Psychologin Maria-Christina Nimmerfroh hält es für falsch die Vereinigung als kriminell abzustempeln, wie es zuvor Politiker von CDU und SPD getan hatten: „Das stärkt deren Gemeinschaft eher statt sie aufzubrechen.“ Sinnvoller sei es etwa darauf hinzuweisen, dass Klebeblockaden noch mehr Staus und Abgase verursachten. Beim Marketing

und der Rekrutierung handle es sich um „eine absolut professionelle Organisation“. Ein so straffes Vorgehen mit Telefon-Marketing, Ansprache vor Ort, raschem Nachfassen und emotionaler Bindung sowie Betreuung sei im zivilgesellschaftlichen Bereich selten (Krempl, „Super-GAU“: Datenschützer nehmen Letzte Generation nach Leck ins Visier, www.heise.de 10.02.2023, Kurzlink: https://heise.de/-7491287).

Niedersachsen

Denis Lehmkemper folgt Barbara Thiel

Die offizielle achtjährige Amtszeit der niedersächsischen Datenschutzbeauftragten Barbara Thiel war Ende 2022 abgelaufen. Die 67-Jährige mit CDU-Parteibuch hatte danach erklärt: „Ich würde gern weiter tätig sein.“ Doch daraus wurde nichts außer einer kurzfristigen Verlängerung um ein halbes Jahr.

Denis Lehmkemper, bisher Leiter der Abteilung für Raumordnung, Landesentwicklung und Förderung im Agrarministerium, wurde am 03.05.2023 vom Landtag in Hannover zum neuen Datenschutzbeauftragten des Landes gewählt. Die Landesregierung schlug den 50-jährigen Juristen, der der CDU angehört, dem Parlament vor – zur Wahl braucht er die Zustimmung von zwei Dritteln der anwesenden Abgeordneten. Lehmkemper hat lange im Innenministerium, in der CDU-Landtagsfraktion, in der Staatskanzlei und im Agrarministerium gearbeitet, er gilt als Fachmann im Personalrecht und Verwaltungsexperte. Mit Lehmkempers Wahl bekommt Agrarministerin Miriam Staudte die Chance eine der vier Abteilungsleiterstellen ihres Hauses neu zu besetzen. Lehmkemper soll nach einem Vorschlag von Ministerpräsident Stephan Weil unter Wegfall seiner Bezüge als Lebenszeit-Beamter beurlaubt werden. Das heißt, dass er nach Ende seiner achtjährigen Amtszeit als Datenschutzbeauftragter wieder in den Landesdienst zurückkehren könnte (Wallbaum, Neuer Datenschutzbeauftragter: Lehmkemper soll am Mittwoch gewählt werden, https://www.rundblick-niedersachsen.de 27.04.2023; Wallbaum, Datenschutzbeauftragte Thiel steht für eine zweite Amtszeit zur Verfügung – und wundert sich, https://www.rundblick-niedersachsen.de 30.01.2023).

Datenschutznachrichten aus dem Ausland

Europa

EDSA macht Weg für TDPF frei

In einer Stellungnahme des Europäischen Datenschutzausschusses (EDSA) äußerte dieser sich verhalten positiv zum 2022 ausgehandelten „Transatlantic Data Privacy Framework“ (TDPF) zwischen der EU und den USA, so der Bundesdatenschutzbeauftragte Ulrich Kelber: „Wir sehen den Willen ein angemessenes Schutzniveau für Betroffene, deren personenbezogenen Daten an Unternehmen in die USA übermittelt werden, zu schaffen.“ Der EDSA äußerte sich aber kritisch zu dem Text der sog. Angemessenheitsentscheidung der EU-Kommission, mit der den USA ein zwar nicht identisches, aber vergleichbares Schutzniveau für die Verarbeitung personenbezogener Daten bescheinigt werden soll.

Dem neuerlichen Anlauf ging mehr als ein Jahr an Verhandlungen voraus. In den USA gibt es weiterhin kein bundeseinheitliches Datenschutzrecht. Die Biden-Regierung änderte zum einen über sogenannte Präsidialverfügungen die Ausführungsbestimmungen für Gesetze, etwa im Bereich der Datenverarbeitung durch Nachrichtendienste, und die Bedingungen, unter welchen diese und die Strafverfolgungsbehörden Daten überhaupt sammeln, auswerten und weitergeben dürfen und ob es gegen Sammlungen gangbare juristische Wege für EU-Bürger gibt dagegen vorzugehen. Damit sollte den Bedenken des EuGH begegnet werden. Die eigentliche Gesetzeslage wurde dabei jedoch nicht angepasst, da es hierfür bislang keine politischen Mehrheiten im Repräsentantenhaus der USA gab. Entsprechend mussten die EU-Datenschutzbehörden nun prüfen, ob die Zusicherungen und zusätzlich übersandte Erläuterungen der US-Regierung eine ausreichende Grundlage für den Angemessenheitsbeschluss bieten können.

In ihrer umfangreichen Stellungnahme erheben die Datenschützer Einwände sehr unterschiedlicher Tragweite, die der Kritik an den Vorgängern Privacy Shield und Safe Harbor in mancher Hinsicht gleichkommt. Deutliche Verbesserungen sehen die Datenschützer beim Zugang zu Rechtsbehelfen, also wenn Nutzer gegen mutmaßliche Verstöße gegen die US-Zusicherungen diese prüfen lassen wollen. Problematisch bleibt aus Sicht der Datenschutzaufsichtsbehörden hingegen, dass Massenerfassungen auf Basis des berühmt-berüchtigten Foreign Intelligence Surveillance Act (FISA) weiterhin ohne Genehmigungsvorbehalt eines richterartigen Gremiums stattfinden dürfen. Bei anderen Kritikpunkten fordern die Datenschützer von der EU-Kommission weitere Informationen ab, doch insgesamt ist das Ergebnis der Prüfung überraschend positiv.

Der Hamburgische Datenschutzbeauftragte Thomas Fuchs begrüßte, dass damit der Weg für die Angemessenheitsentscheidung frei scheint: „Im Zuge der Verhandlungen haben die USA bisher nicht dagewesene Zugeständnisse gemacht und ihr nationales Sicherheitsrecht an europäische Grundrechtsmaßstäbe angepasst.“ Der Beschluss des EDSA sei aber kein Freibrief: „Ob und inwiefern tatsächlich Geheimdienstaktivitäten auf ein verhältnismäßiges Maß reduziert werden und wirksamer Rechtsschutz gewährleistet ist, kann nur die Umsetzung in der Praxis zeigen.“ Die europäischen Datenschutz-

behörden hatten der Kommission unter anderem eine strenge Überwachung der tatsächlichen Umsetzung als Maßgabe mit auf den Weg gegeben – so sollte die Kommission etwa spätestens alle drei Jahre eine grundsätzliche Überprüfung des TDPF durchführen.

Der Angemessenheitsbeschluss dürfte nun die weiteren Instanzen passieren; das Europaparlament könnte ihn nur mit absoluter Mehrheit zurückweisen. Das scheint nach der EDSA-Stellungnahme allerdings ausgeschlossen. Wenn die noch ausstehenden formellen Schritte vollzogen sind und der Angemessenheitsbeschluss in Kraft ist, können sich Unternehmen auf die neue Rechtsgrundlage berufen.

Damit Unternehmen dann personenbezogene Daten unter den Regeln des Transatlantic Data Privacy Framework in die USA übertragen und dort verarbeiten dürfen, müssen diese sich einem speziellen Aufsichtsregime der US-Handelsaufsicht (Federal Trade Commission – FTC) oder des Handelsministeriums (Department of Commerce – DoC) unterwerfen. Hierzu müssen sie ihre Teilnahme anmelden. Sofern sie die Kriterien nicht erfüllen, drohen bei Selbstverpflichtungsverstößen in den USA oft empfindliche Strafen (Steiner, Europas Datenschützer machen Weg für EU-US-Datenschutzvereinbarung frei, www.heise.de 02.03.2023, Kurzlink: https://heise.de/-7532414).

Frankreich

„Intelligente“ Videoüberwachung bei Olympiade 2024 in Paris

Das französische Parlament hat am 23.03.2023 im Kern einen Gesetzentwurf der Regierung gebilligt, der einen breiten Einsatz von Kameras zur „intelligenten“ Videoüberwachung in Echtzeit während der Olympischen Sommerspiele 2024 in Paris vorsieht. Das System soll selbstständig Ereignisse wie Menschenansammlungen erfassen und auf eventuelle Gefahren hin analysieren. So soll dem Gesetzestext zufolge die Sicherheit von „Sport-, Freizeit- oder Kulturveranstaltungen“ gewährleistet werden. Der Senat hatte bereits zuvor zugestimmt. Die Olympischen Sommerspiele 2024 finden vom 26.07. bis zum 11.08.2024 in Paris statt. Vom 28.08. bis zum 08.09.2024 ist die französische Hauptstadt Austragungsort der Paralympics. Entgegen der ursprünglichen Vorlage soll das Überwachungsprogramm bis zum 24. Dezember 2024 laufen statt bis Juni 2025.

Vor der Abstimmung der Rechtspolitiker waren 37 zivilgesellschaftliche Organisationen wie European Digital Rights (EDRi), La Quadrature du Net, Amnesty International, Digitalcourage, die DVD und Privacy International in einem Brandbrief gegen das Vorhaben Sturm gelaufen. Dieses ebnet ihnen zufolge „den Weg für den Einsatz von invasiver, Algorithmen-gesteuerter Videoüberwachung unter dem Vorwand Großveranstaltungen zu sichern“. Mit dem Gesetz würde Frankreich der erste EU-Mitgliedsstaat, „der solche Praktiken ausdrücklich legalisiert“ (siehe in diesem Heft S. 96).

Die Bürgerrechtler befürchten, dass die Initiative den Weg für eine biometrische Massenüberwachung ebnet. Nur selten würden einmal eingeführte „außergewöhnliche“ Maßnahmen tatsächlich wieder zurückgenommen. Stattdessen erschiene die Überwachung als neue Normalität – oft ohne angemessene Schutzmaßnahmen, Transparenz, Einbeziehung der Betroffenen und Mechanismen der Rechenschaftspflicht. Der Aufforderung, den die Videoüberwachung legitimierenden Artikel 7 abzulehnen und das Thema für weitere Diskussionen mit der Zivilgesellschaft zu öffnen, kam die Nationalversammlung nicht nach.

Mit dem Ansatz will die Regierung es den Sicherheitsbehörden ermöglichen „verdächtiges Verhalten“, unbeaufsichtigtes Gepäck und große Menschenansammlungen alarmierenden Ausmaßes zu erkennen. Mehrere Abgeordnete und Fraktionen drängten darauf auch eine Live-Gesichtserkennung zuzulassen. Sie fanden damit aber genauso wenig eine Mehrheit wie rund 90 Parlamentarier aus dem linken Spektrum, die sich gegen Artikel 7 des Gesetzes aussprachen. Das Parlament stimmte aber dafür die Öffentlichkeit besser über die Standorte der Kameras zu informieren und neben der Datenschutzbehörde CNIL auch die Cybersicherheitsagentur ANSSI einzubeziehen. Ferner hat das Gremium den Fundus an Bildern und Daten erweitert, mit denen Algorithmen im Vorfeld der Wettbewerbe trainiert werden können.

Die Bürgerrechtsorganisation „La Quadrature du Net“ wirft der französischen Regierung vor nicht wahrheitsgetreu über die technische Funktionsweise und die rechtlichen und politischen Konsequenzen informiert zu haben. Stattdessen seien „Strategien, Lügen und erfundene Darstellungen“ eingesetzt worden, um Diskussionen über die geplante Massenüberwachung zu verhindern (Krempl, Warnung vor Big-Brother-Olympiade verhallt im französischen Parlament, www.heise.de 09.03.2023, Kurzlink: https://heise.de/-7540846; Frankreich: Parlament beschließt umstrittene Videoüberwachung zu Olympia, https://posteo.de 27.03.2023).

Italien

Datenschutzbehörde gegen OpenAIs ChatGPT

Die italienische Datenschutzaufsichtsbehörde, die „Garante per la protezione dei dati personali“, ging unter Berufung auf Art. 58 Datenschutz-Grundverordnung (DSGVO) mit einer vorübergehenden Sperrung „mit sofortiger Wirkung“ landesweit gegen ChatGPT vor und nimmt weitere Untersuchungen vor. Ein Grund dafür ist, dass OpenAI unrechtmäßig personenbezogene Daten verarbeitet. Sie ist damit erste Behörde der Welt, die die Nutzung von ChatGPT auf der Grundlage von Datenschutzbestimmungen blockiert.

Als Basis für die Anschuldigungen dient maßgeblich ein am 20.03.2023 aufgetauchtes Datenleck, das die Einsicht in die Informationen fremder Nutzer erlaubte; sogar Zahlungsdaten waren dabei. Das Leck betraf Unterhaltungen der Nutzer mit der Anwendung sowie Informationen über die Bezahlung der Abonnenten des kostenpflichtigen Dienstes. OpenAI-Chef Sam Altman hatte erklärt, das Datenleck habe einen Fehler in einer Open-Source-Bibliothek als Ursache gehabt. Konkreter wurde er dabei allerdings nicht. Die Behörde

teilte mit: „In der Maßnahme stellt die Datenschutzaufsichtsbehörde fest, dass die Nutzer und alle Personen, deren Daten von OpenAI gesammelt werden, nicht informiert wurden, vor allem aber, dass es keine Rechtsgrundlage gibt, die die massive Sammlung und Speicherung personenbezogener Daten zum Zwecke des ‚Trainings' der Algorithmen, die dem Betrieb der Plattform zugrunde liegen, rechtfertigt." Guido Scorza, ein Vertreter der Behörde, erklärte: „Wer medizinische Forschung betreibt, muss die Zustimmung für Experimente einholen. Diejenigen, die mit neuen Technologien experimentieren, müssen den Prozess ebenfalls transparent machen."

Der Einsatz von Nutzungsdaten aus Italien wurde untersagt. Problematisch ist aber jegliche Nutzung von Eingaben von Nutzerinnen und Nutzern, die zum Training der Künstlichen Intelligenz genutzt werden.

Außerdem behauptete die Garante, dass Überprüfungen Diskrepanzen zwischen den von ChatGPT bereitgestellten Informationen und den tatsächlichen Daten ergeben hätten. ChatGPT liefere häufig fehlerhafte Antworten; darin liegt nach Ansicht der Behörde „eine unzulässige Verarbeitung personenbezogener Daten". Ein weiterer Kritikpunkt betrifft das Mindestalter: OpenAI gibt ChatGPT in seinen Nutzungsbedingungen für Menschen ab 13 Jahren frei, überprüft das Alter in der Web-App aber nicht. Junge Leute könnten so ungeeignete Antworten erhalten, die nicht für ihr Alter bestimmt sind: „Das Fehlen eines Filters zur Überprüfung des Alters der Nutzer führt dazu, dass Minderjährige Antworten erhalten, die für ihren Entwicklungsstand und ihr Selbstbewusstsein völlig ungeeignet sind". Fehlende Alterskontrollen sind allerdings keine Seltenheit, die meisten sozialen Netzwerke prüfen nur wenig verlässlich.

Innerhalb von 20 Tagen nach der Verfügung sollte das Unternehmen mitteilen, welche Korrekturmaßnahmen es ergriffen hat. Ansonsten drohe eine Strafe von bis zu 20 Millionen Euro oder bis zu 4% des globalen Jahresumsatzes, so die Behörde. OpenAI könne Widerspruch einlegen; das Unternehmen müsse der Anweisung der Behörde aber zunächst nachkommen.

Nach der Sperrverfügung durch die italienische Datenschutzaufsichtsbehörde ließ sich ChatGPT als Web-App beim Entwicklerunternehmen OpenAI per VPN-Tunnel noch mit italienischer IP aufrufen. Die Garante war im Februar bereits in ähnlicher Weise gegen einen anderen Chatbot mit dem Namen Replika vorgegangen. Dabei ging es vor allem darum, dass Kinder im Alter unter 13 Jahren ungenügend geschützt wurden.

Nach Änderungen seines Internetauftritts war ChatGPT in Italien am 28.04.2023 wieder verfügbar. Die Garante erklärte: „OpenAI stellt den Dienst in Italien mit verbesserter Transparenz und verbesserten Rechten für europäische Benutzer wieder her." Das Unternehmen erfülle nun eine Reihe von Bedingungen, die die Behörde gefordert hatte, um das Verbot des Chatbots aufzuheben. Der Betreiber OpenAI gab bekannt unter anderem eine Altersprüfung für einheimische neue Nutzer vorgeschaltet zu haben. Ein neues Formular erlaube es Nutzern in der Europäischen Union zudem Widerspruch gegen die Verwendung ihrer Daten einzulegen. Die italienische Datenschutzbehörde erklärte, sie werde jedoch die Datenschutzprüfung fortsetzen und forderte weitere Maßnahmen.

In Deutschland sind die unabhängigen Datenschützer:innen der Länder für Unternehmen zuständig (s.o. S. 102). Eine Sprecherin des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) erklärte, dass man mit der italienischen Datenschutzaufsichtsbehörde „sehr eng" zusammenarbeite: „Wir haben sie zur Sperrung von ChatGPT bereits um weiterführende Informationen gebeten und werden diese dann an die zuständigen Landesdatenschutzaufsichtsbehörden und Landesmedienanstalten weitergeben."

ChatGPT basiert darauf, dass die Software enorme Mengen von Texten erfasst und auf dieser Basis Texte erstellt, die von denen eines Menschen kaum zu unterscheiden sind. Dabei schätzt das Programm nach einer statistischen Methode, welche Worte als nächste in einem Satz folgen könnten. Das Prinzip hat zur Folge, dass die Software „Fakten halluziniert", wie OpenAI es nennt, also falsche Informationen auswirft. ChatGPT hat seit Ende 2022 damit beeindruckt, wie gut die Software menschliche Sprache imitiert. An Schulen und Hochschulen besteht das Problem, dass damit Hausaufgaben und Arbeiten produziert werden können, die keine Leistung der Schüler und Studierenden sind (Sokolow, Italiens Datenschützer stoppen ChatGTP, Kieler Nachrichten, 01.04.2023, 5; Mantel, Datenschutzbedenken: Italien will ChatGPT sperren, www.heise.de 31.03.2023, Kurzlink: https://heise.de/-8326147; Schubert, Italien sperrt ChatGPT, www.faz.net 31.03.2023; Italiens Datenschutzbehörde sperrt ChatGPT, Tagesspiegel Digitalisierung & KI 03.04.2023; ChatGPT in Italien wieder verfügbar, www.tagesschau.de 28.04.2023; Wittenhorst, Text-KI ChatGPT in Italien wieder verfügbar, www.heise.de 29.04.2023, Kurzlink: https://heise.de/-8983351).

Schweiz

„Anonyme" Gesichtserkennung auf Schweizer Bahnhöfen

Reisende und Passanten auf vielen Bahnhöfen der staatseigenen Schweizerischen Bundesbahnen (SBB) werden bereits vielfach gefilmt und getrackt, sei es mit Hunderten Videokameras, sei es beim Benutzen der Fahrkartenautomaten oder mithilfe eines Systems zum Messen von Personenströmen. Im Laufe des Jahres 2023 soll zunächst am Bahnhof Schaffhausen ein weiteres Überwachungssystem mit „anonymisierter Gesichtserfassung" hinzukommen. Das Schweizer Konsumentenschutz-Magazin K-Tipp hat einen Beschaffungsplan für ein „Kundenfrequenz-Messsystem 2.0" auf einer Ausschreibungsplattform entdeckt, welches ein Gesichtserfassungssystem einschließt. Kamerasysteme mit Gesichtserfassung und -erkennung im öffentlichen Raum werden auch in der Schweiz seit geraumer Zeit diskutiert und zumeist abgelehnt.

Das neue System, das für 57 Schweizer Bahnhöfe geplant ist, soll nicht nur wie bisher die Bewegungen der Personen im Bahnhofsbereich tracken. Die SBB wollen laut K-Tipp außerdem das (Kauf-) Verhalten der Passanten in den zahlreichen Ladengeschäften und Lokalen der

größeren Bahnhöfe beobachten. Die so gewonnenen Einblicke – nebst Verbindung mit anderen Quellen wie Wetter- und Fahrgastdaten – will die Bahn mit den Daten des Swisspass (eine SBB-Kundenkarte mit Bild) verknüpfen.

Erfasst werden sollen die Daten von den meist verdeckt angebrachten Kameras. Damit erkundet werden sollen Alter und Geschlecht der Personen, die Größe, mitgeführtes Gepäck und Gegenstände wie Kinderwagen, Rollstuhl, Fahrrad oder begleitende Tiere. Die SBB interessieren sich dafür, wie lange Reisende sich im Bahnhof aufhalten, welche Läden Passagiere besuchen und wie viel Geld sie dort ausgeben. Auch die Daten der Ladenkassen wollen die SBB mit den Bewegungsdaten verbinden und damit offenbar die „Abschöpfungsrate" pro Passagier erhöhen: Je höher der Umsatz der Läden in den Bahnhöfen, desto höher fällt die Miete aus, die diese an die SBB entrichten müssen. Die Ladenbetreiber sollen Zugang zu den Informationen erhalten. Die erste Variante des Kundenfrequenz-Messsystems war wohl 2017 in einzelnen Bahnhöfen installiert worden; sie zeichnete gemäß Presseberichten die Position von Personen auf und wies diesen zusätzlich zu ihrem Standort und dem Zeitpunkt der Aufnahme eine Identität zu, die über den gesamten Erfassungszeitraum konstant blieb.

Zwecks Einhaltung des Datenschutzrechts verlangen die SBB vom Systemlieferanten, dass die Daten anonymisiert erhoben werden. Allerdings solle eine Personen-ID vergeben werden, damit Personen „während der gesamten Aufenthaltsdauer im Bahnhof eindeutig erkannt werden können". Schon damals – wie auch heute – betonten die SBB, dass trotz solch einer „eindeutigen Identifikation der Person" Rückschlüsse auf Einzelpersonen nicht möglich seien. Die SBB beteuern, es werde nur mit aggregierten Daten gearbeitet. Die Informationen der Ladenkassen würden nur „allgemein genutzt". Die Personen-ID habe nichts mit der Person zu tun, sondern sei eine rein technische Nummerierung. Es würden keine Daten verknüpft, welche Rückschlüsse auf die Person zulassen, und es gebe keine Verknüpfung mit dem Swisspass oder Mobile-Apps. Der Datenschutz sei gewährleistet. Es werde nichts beschafft und eingesetzt, das nicht datenschutzkonform sei.

Der Eidgenössische Datenschützer (EDÖB), Adrian Lobsiger, meinte, aufgrund der Vielzahl der erhobenen Daten und des Risikos der Re-Identifikation von Personen bestehe eine erhebliche Gefahr für die Persönlichkeit der Passanten. Er bestätigte, dass er von den SBB „im Oktober 2022 über dieses Projekt informiert" wurde. Die SBB „sicherten dem EDÖB zu, dass die Daten nicht personenbezogen verwendet werden, und dass sie eine Datenschutz-Folgenabschätzung zum Projekt durchführen werden. Der EDÖB wird das Projekt weiterhin aufsichtsrechtlich begleiten" (Sperlich, Gesichtserkennung: Kritik an Schweizer Bahn wegen „Kundenbespitzelung", www.heise.de 20.02.2023, Kurzlink: https://heise.de/-7520789).

Schweiz

Doch keine Biometrie-Kontrolle auf Bahnhöfen

Die Schweizerischen Bundesbahnen (SBB) werden in ihrem kommenden neuen Messsystem auf Bahnhöfen die Menschen doch nicht nach Alter, Geschlecht oder Größe erfassen. Die Konzernleitung der SBB gab anlässlich einer Bilanzmedienkonferenz am 13.03.2023 bekannt, dass die staatseigenen SBB nach wie vor zusätzlich zu den bereits Zehntausenden von Kameras, die in Zügen und Bahnhöfen im Einsatz sind, weitere Überwachungssysteme in 57 Bahnhöfen installieren möchten. Sie sollen die Ströme der Reisenden und Kundinnen und Kunden der zahlreichen Geschäfte in den Bahnhöfen erfassen, mit Hilfe des „Kundenfrequenz-Messsystem 2.0" (KFMS) gemäß einem Beschaffungsplan auf einer Ausschreibungsplattform (siehe vorige Meldung).

Nach erheblichem öffentlichem Druck und auch Einwänden aus der Politik modifizierten die SBB die angeforderten Möglichkeiten in den Ausschreibungsplänen. Das Bahnunternehmen verkündete keine Gesichtserkennung in den Bahnhöfen einsetzen zu wollen und auch keine Daten zu erheben, die Rückschlüsse auf einzelne Personen ermöglichen. Im hauseigenen Newsportal war nach Veröffentlichung der ersten Kritik im Februar 2023 zunächst mitgeteilt worden: „Die Ausschreibung war sehr technisch formuliert und stellenweise schlicht missverständlich. Das müssen wir künftig besser machen." An dem Plan der ausgeschriebenen Kundensegmentierungen wie Alter, Geschlecht oder Größe werde aber festgehalten. Später zog dann aber die Konzernleitung, allen voran wohl SBB-Chef Vincent Ducrot, die Notbremse. Er will auf die Kundenkategorisierungen verzichten. Zwar hätten die SBB nur ein System beschafft, das vollständig datenschutzkonform sei, so Ducrot: „Der Nutzen für das Kerngeschäft Bahn ist für mich jedoch zu wenig gegeben." Zudem habe er die Befürchtungen aus Politik und Öffentlichkeit gehört und ernst genommen: „Das Vertrauen in die SBB ist mir sehr wichtig."

Die SBB unterstreichen nun, dass bei den Zähldaten keine Verknüpfungen mit Personendaten gemacht würden. Ziel sei, „dass sich die Reisenden, alle Besucher:innen im Bahnhof sicher und wohl fühlen und die richtigen Services am richtigen Ort sind." Die SBB würden ihre Ausschreibung anpassen. Für eingehende Angebote werde eine Datenschutz-Folgenabschätzung erstellt. Erst nach Prüfung durch den Eidgenössischen Datenschutzbeauftragten (EDÖB) wollen sich die SBB für ein Angebot entscheiden. Gegen die Pläne der SBB haben die beiden zivilgesellschaftlichen Organisationen AlgorithmWatch CH und die Digitale Gesellschaft gemeinsam mit anderen Organisationen einen offenen Brief lanciert, der von über 16.000 Personen unterzeichnet wurde. Darin wurde gefordert „auf biometrische Kategorisierung und Überwachung zu verzichten". Die beiden Organisationen „begrüßen die Ankündigung der SBB", betonen aber gleichzeitig, dass sie den Druck aufrechterhalten und den SBB weiterhin genau auf die Finger schauen möchten, damit auch in Zukunft keine Überwachungsmethoden eingesetzt werden, die mit den Grundrechten nicht vereinbar sind (Sperlich, Schweizer Bahn verzichtet auf biometrische Überwachung der Bahnhöfe, www.heise.de 15.03.2023, Kurzlink: https://heise.de/-7547175).

Dänemark

Kundendaten von Ecco öffentlich im Netz

Ecco, ein dänisches Schuh- und Bekleidungsunternehmen, hat nach Drohungen von Anonymous 60 GB mit Millionen sensibler Daten preisgegeben, die von Sicherheitsexperten des dänischen Cybersicherheitsunternehmens PrivacySharks am 21.12.2022 entdeckt wurden. Die Daten sollen seit Juni 2021 öffentlich zugänglich gewesen sein.

Ecco verwendete zur Visualisierung seiner Daten Kibana, worüber wegen einer Schwachstelle durch eine offene API auf Kundendokumente zugegriffen werden konnte. Die Dokumente enthalten Verkaufs- und Marketingmaterial bis hin zu Protokollierungs- und internen Systeminformationen. Für einen Wettbewerber wären die 190.005 Dokumente, die als aboservice_asset_availability_check kategorisiert sind, und die 305.508 Dateien, die als sales_org kategorisiert sind, von großem Wert, weil sie einen einzigartigen Einblick in das Geschäft von Ecco bieten. Neben dem Zugriff auf die Daten bestand auch die Möglichkeit die Kodierung zu ändern, die schließlich mit der Ecco-Website verbunden wurde.

Die Daten wurden von Anonymous veröffentlicht. PrivacySharks erklärte: „Es ist ein Wunder, dass Anonymous, das Ecco schon früher bedroht hat, diese Lücke nicht vor den Experten gefunden hat.“ Ob die Daten missbraucht wurden und Auswirkungen auf die Zukunft der internen Systeme von Ecco haben, ist ungewiss. Das Sicherheitsunternehmen empfiehlt Benutzern ihr Passwort zu ändern und einen Passwortmanager zu verwenden. Ecco hat die Lücke inzwischen geschlossen (Sørensen, Truet af Anonymous, danske Ecco lækker over 60GB sensitiv data, www.privacysharks.com/dk/author/rasmus-soerensen/ 22.12.2022).

Großbritannien

Sammelklage gegen Meta vorläufig gescheitert

Das britische Competition Appeal Tribunal (CAT) hat am 20.02.2023 in London eine Sammelklage gegen Meta mit einem Streitwert von bis zu drei Milliarden Pfund (rund 3,4 Milliarden Euro) abgewiesen. In der Klage wurde dem Social-Media-Konzern vorgeworfen seine marktbeherrschende Stellung bei Facebook zu missbrauchen, um die persönlichen Daten der Nutzer und Nutzerinnen zu Geld zu machen. Das Gericht räumte den Klägern jedoch bis zu sechs Monate Zeit ein, um einen weiteren Versuch zu unternehmen den angeblichen Schaden für die Nutzer und Nutzerinnen nachzuweisen.

Die im Namen von rund 45 Millionen Facebook-Nutzenden in Großbritannien eingereichte Sammelklage gegen die Facebook-Muttergesellschaft Meta war von der Wettbewerbsexpertin Liza Lovdahl Gormsen vom British Institute of International and Comparative Law eingereicht worden. Lovdahl Gormsen argumentiert, die Facebook-Nutzenden würden nicht angemessen für den Wert der persönlichen Daten entschädigt, die sie für die Nutzung des Sozialen Netzwerkes bereitstellen mussten. Das CAT, das für kartellrechtliche Verfahren zuständig ist, entschied, dass die der Klage zugrundeliegende Methode zur Ermittlung der von den Facebook-Usern erlittenen Verluste einer „grundlegenden Neubewertung“ bedürfe, damit der Fall fortgesetzt werden könne. Das Londoner Gericht gab den Anwälten von Lovdahl Gormsen jedoch sechs Monate Zeit, um „zusätzliche Beweise einzureichen, die einen neuen und besseren Plan für einen effektiven Prozess darstellen“. Ein Sprecher von Meta begrüßte die Entscheidung und verwies auf eine frühere Erklärung, wonach die Klage „völlig unbegründet“ sei.

Das CAT hat mit mehreren Sammelklagen gegen große Unternehmen wie BT, Apple, Qualcomm oder Sony zu tun. Der japanische Elektronik-Konzern soll seine marktbeherrschende Stellung missbraucht haben, um den Entwicklern und Verlegern von PlayStation-Spielen unfaire Bedingungen aufzuerlegen. Eine weitere Sammelklage fordert eine Milliarden-Entschädigung wegen Apples umstrittener App-Store-Regeln. Ermöglicht werden solche Kartellklagen im Namen von Millionen von Verbrauchern wegen angeblicher Verstöße gegen das Wettbewerbsrecht durch den britischen Consumer Rights Act von 2015. Jede Klage muss zunächst vom CAT als verhandlungsfähig bestätigt werden.

Ende 2020 hat der Oberste Gerichtshof ein wegweisendes Urteil gefällt, durch das eine Klage des ehemaligen Finanzombudsmanns Walter Merricks im Namen von 46,2 Millionen Menschen gegen den Finanzdienstleister Mastercard in Höhe von 10 Milliarden Pfund (11,8 Milliarden Euro) zugelassen wurde (Knobloch, Facebook: Sammelklage in Großbritannien abgewiesen, www.heise.de 20.02.2023, Kurzlink: https://heise.de/-7521997).

USA

Private Kfz-Videos vergnügen Tesla-Mitarbeiter

Von 2019 bis zumindest 2022 haben gemäß einem Bericht von Reuters Tesla-Mitarbeitende Originalszenen sowie bearbeitete Aufnahmen aus den Kameras fremder Tesla-Fahrzeuge in einem Firmenchat geteilt und sich darüber lustig gemacht. Zu den Bildern gehörten intime Szenen in Garagen, Autos und Privatgärten bis zu furchtbaren Straßenunfällen. Der Bericht bezieht sich auf Angaben von neun ehemaligen Tesla-Mitarbeitern. Einige weitere Befragte wollten nichts mitbekommen haben. Ob die Praxis andauert, ist nicht geklärt. Besonders beliebt gewesen sei ein Video eines Rasers, der ein fahrradfahrendes Kind verletzte. Auch Nacktaufnahmen oder ein Amphibienfahrzeug aus der Garage des Tesla-Chefs Elon Musk erregten demnach firmeninterne Aufmerksamkeit.

Ein Teil der Aufnahmen sei entstanden, während das jeweilige Elektroauto nicht in Betrieb war. Manche Fotos und Videos wurden über Gruppenchats verteilt, andere über Unterhaltungen mit wenigen Teilnehmern – das auch dann, wenn ein Manager die Verbreitung im Gruppenchat als Verletzung interner Vorschriften gerügt hatte. Tesla war nach der Veröffentlichung für Stellungnahmen nicht erreichbar. Tesla verspricht: „Your Data belongs to you.“ Autobesitzer sollen via Touchscreen selbst entscheiden, ob sie Daten ihrer Tesla-Autos dem Hersteller für Analysezwecke freigeben möchten: „Diese

Analyse hilft Tesla seine Produkte und Dienstmerkmale zu verbessern sowie Probleme schneller zu diagnostizieren."

Fotos und Videos würden weder mit dem Autokäufer noch der Fahrgestellnummer verknüpft. Letzteres stimmt offenbar; allerdings sind die Aufnahmen stets georeferenziert. Tesla-Mitarbeiter hätten durch einen Link auf Google Maps nachschauen können, wo die Aufnahme gemacht wurde. In Verbindungen mit dem Gezeigten ist es dann keine Schwierigkeit Bezug zu bestimmten Personen herzustellen. Die Einstellung der Tesla-Mitarbeiter war in den Gesprächen mit Reuters unterschiedlich. Zwei hätten nichts dabei gefunden die Aufnahmen aus fremden Autos zu teilen. Die Kunden hätten sowieso jede Erwartung von Privatsphäre aufgegeben. Ein Weiterer hatte keine grundsätzlichen Bedenken, stufte aber die Verbindung mit dem Ort der Aufnahme als „massives Eindringen" ein. Drei andere Ex-Tesla-Leute zeigten sich hingegen beunruhigt mit Kommentaren wie: „Es war eine Verletzung der Privatsphäre, wenn ich ehrlich bin." Oder: „Ich habe immer gescherzt, dass ich nie einen Tesla kaufen würde, nachdem ich gesehen habe, wie sie manche dieser Leute behandeln."

In Reaktion auf den Reuters-Bericht zum Umgang mit Videoaufnahmen aus Kundenfahrzeugen hat der Tesla-Besitzer Henry Yeh bei einem Bezirksgericht in Nord-Kalifornien eine Sammelklage gegen den Autobauer eingereicht (Aktenzeichen 3:23-cv-01704). Yeh klagt in seinem Namen und stellvertretend für alle weiteren Betroffenen. Neben Intim-Fotos und Videos standen bei den Tesla-Mitarbeitern wohl auch Videos zu Unfällen und Ärger im Straßenverkehr hoch im Kurs. Sollten die Richter in den USA die Klage anerkennen, dann kann Tesla zur Zahlung von Schadensersatz an Fahrzeugbesitzer verpflichtet werden. Laut dem Kläger hätten die Besitzer eines Tesla derzeit zwar die Möglichkeit die Kameras von einer Fachkraft deaktivieren zu lassen, würden dabei aber den Zugriff auf den Autopiloten verlieren. Die Fahrassistenz der Elektroautos ist eines der schlagenden Verkaufsargumente. Für den Fall, dass man die Kameras angestellt lasse, müsse man im Zweifel damit rechnen, dass die eigene Privatsphäre nicht geschützt sei (Stecklow/Cunningham/Jin, Special Report: Tesla workers shared sensitive images recorded by customer cars, www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/; Sokolov, Tesla-Mitarbeiter ergötzen sich an Videoaufnahmen aus fremden Autos, www.heise.de 07.04.2023, Kurzlink: https://heise.de/-8688648; Steevens, Tesla: Späße mit Kundenvideos führen zu Sammelklage, www.heise.de 09.04.2023, Kurzlink: https://heise.de/-8854871).

Kanada

Datenschutz ermittelt gegen OpenAIs ChatGPT

Das Büro des Datenschutzbeauftragten von Kanada hat eine Untersuchung gegen OpenAI eingeleitet. Das Unternehmen entwickelt den mit künstlicher Intelligenz betriebenen Chatbot ChatGPT. Philippe Dufresne, Privacy Commissioner of Canada, erläuterte: „Die KI-Technik und ihre Auswirkungen auf die Privatsphäre haben für mein Büro Priorität. Wir müssen mit den schnelllebigen technologischen Fortschritten Schritt halten – und ihnen einen Schritt voraus sein." Damit reagierte der oberste kanadische Datenschützer auf eine Beschwerde. Es geht um die Erhebung, Verwendung und Offenlegung personenbezogener Daten ohne Zustimmung. Weil die Untersuchung noch laufe, würden keine weiteren Details bekanntgegeben.

Im Nachbarland USA hat eine gemeinnützige Forschungsorganisation die dort für Verbraucherschutz zuständige Federal Trade Commission (FTC) aufgefordert gegen OpenAI Ermittlungen einzuleiten. In Italien wurde auf Betreiben der dortigen Datenschutzaufsicht der Zugang zu ChatGPT zeitweise gesperrt (s.o. S. 107). IT-Unternehmen in Südkorea bemühen sich laut einem Bericht der Korea Times darum ihren Mitarbeitern Richtlinien im Umgang mit ChatGPT aufzuerlegen. Da diese den Chatbot nutzten, um beispielsweise zu programmieren oder ihre Meetings zu organisieren, bestehe das Risiko, dass Geschäftsgeheimnisse an die Öffentlichkeit dringen.

In einem vom Future of Life Institute (FLI) veröffentlichten Manifest hatten über 10.000 teils prominente Unterzeichnerinnen und Unterzeichner wie Elon Musk und Steve Wozniak eine halbjährige Zwangspause für die Arbeit an KI-Modellen gefordert, die „mächtiger als GPT-4" seien. Nur so könne man gewährleisten, dass die KI zum Wohle der Menschheit beitrage statt ihr zu schaden (Wilkens, ChatGPT: Kanadische Datenschutzbehörde untersucht OpenAI, www.heise.de 06.04.2023, Kurzlink: https://heise.de/-8654196)

Kanada

Schwaches Datenschutzrecht lässt Meta im Cambridge Analytica-Rechtsstreit obsiegen

Die vom kanadischen Bundesdatenschutzbeauftragten verhängten Auflagen für Facebook-Betreiber Meta Platforms im Zusammenhang mit dem Cambridge Analytica-Skandal sind gemäß dem Spruch des Federal Court in Ottawa im Verfahren „Privacy Commissioner of Canada v. Facebook" vom 13.04.2023 nichtig (Az. 2023 FC 533). Der Bundesrichter sprach deshalb Meta 80.000 kanadische Dollar (rund 55.000 Euro) als Ersatz für die Verfahrenskosten zu. Der im Jahr 2018 bekannt gewordene Datenmissbrauch durch Cambridge Analytica gehört zu den größten Skandalen in der Geschichte Facebooks. Das inzwischen insolvente britische Unternehmen Cambridge Analytica war auf regelwidrige Weise an Daten von 87 Millionen Facebook-Nutzern gelangt: Es hatte eine „Umfrage"-App unter dem Namen thisisyourdigitallife (TYDL) veröffentlicht, an der Facebook-Nutzer teilnahmen. Dank der Privatsphäre-Einstellungen des Datenkonzerns bekam Cambridge Analytica Zugang zu Informationen von deren Facebook-Freunden, die in der Folge für manipulative Polit-Kampagnen missbraucht wurden.

Als das bekannt wurde, geriet Facebook, dessen Management sich in dem Datenskandal selbst als Opfer darstellte, massiv in die Kritik und gelobte Besserung beim Datenschutz. Es folgten verschiedene Verfahren. In den USA muss-

te Facebook fünf Milliarden US-Dollar Strafe zahlen – die höchste Strafe in der Geschichte der US-Handelsbehörde FTC (Federal Trade Commission, DANA 3/2019, 164 f.). Eine Sammelklage in dem Land mündete in eine Vergleichszahlung Metas von 725 Millionen Dollar. In Großbritannien wurde dem Konzern die geringe Höchststrafe von einer halben Millionen Pfund verhängt (DANA 4/2018, 210), in Italien kam es zu einem Bußgeld in Höhe von 1,1 Millionen Euro.

In Kanada konnte die Bundesdatenschutzaufsicht OPC (Office of the Privacy Commissioner) keine Strafe verhängen, sondern nur Empfehlungen aussprechen. Facebook solle 1. den Zugriff Dritter auf nicht benötigte Daten einschränken, 2. Nutzer darüber informieren, welche Informationen eine Anwendung benötige und für welchen Zweck und 3. die Zustimmung der Nutzer zur Übertragung dieser Daten einholen.

Selbst gegen diese Minimalauflagen wehrte sich Meta mit Erfolg. Gemäß dem Urteil des Bundesgerichts habe die Bundesdatenschutzaufsicht nicht nachgewiesen, dass Facebook keine wirksame Zustimmung der Nutzer eingeholt hat. Es gäbe ein „Beweisvakuum“, obwohl Facebook selbst behauptete, von Cambridge Analytica hinters Licht geführt worden zu sein: Wenn Facebook schon nicht weiß, welche Daten wofür abkopiert wurden, ist schwer ersichtlich, wie es wirksame Zustimmung seiner User eingeholt haben könnte.

Zudem sei Facebook nach kanadischem Datenschutzrecht nicht verpflichtet die Nutzerdaten zu schützen, sobald sie an Dritte übertragen werden. Der Richter kritisierte dabei das geltende Recht: Es liege am Gesetzgeber „gut durchdachte und ausbalancierte Gesetze, die die durch (...) digitales Teilen personenbezogener Daten gestellten Herausforderungen angehen“, zu schaffen. Das Gericht könne nur bestehendes Recht anwenden, das für Soziale Netzwerke in gleicher Weise greife wie für den lokalen Autohändler. Der kanadische Datenschutzbeauftragte kann selbst keine Strafen verhängen, sondern sie nur bei Gericht beantragen. Dabei liegt die Höchstgrenze derzeit bei mageren 100.000 Dollar (zirka 68.000 Euro).

Im kanadischen Bundesparlament wird derzeit ein Gesetzesantrag namens Bill C-27 behandelt, der Datenschutz verbessern, mögliche Geldstrafen deutlich erhöhen und Betroffenen den Klageweg gegen schludrige Unternehmen eröffnen soll. Allerdings sollen Betroffene nur dann klagen dürfen, wenn der Datenschutzbeauftragte Kanadas oder ein neues Datenschutztribunal bereits rechtskräftig festgestellt hat, dass Datenschutzrecht verletzt wurde. Eine solche Feststellung kann – wie im vorliegenden Fall – Jahre dauern. Verbraucher können eine Untersuchung nicht erzwingen. Hat der Datenschutzbeauftragte Kanadas also keine Kapazität oder Lust, sich mit einem bestimmten Fall auseinanderzusetzen, bleibt dessen Opfern der Klageweg auch nach der beabsichtigten Gesetzesnovelle versperrt (Sokolov, Kanadas Datenschutz scheitert an Cambridge Analytica, www.heise.de 18.04.2023, Kurzlink: https://heise.de/-8969386; vgl. auch DANA 1/2019, 46).

Rechtsprechung

EGMR

Schadenersatz für Whistleblower in Lux-Leaks-Affäre

Die Große Kammer des Europäischen Gerichtshofs für Menschenrechte (EGMR) mit ihren insgesamt 17 Richterinnen und Richtern hat mehrheitlich im Verfahren um den Whistleblower Raphael Halet am 14.02.2023 entschieden, dass die Gerichte in Luxemburg ihn zu Unrecht verurteilt haben und er daher vom Staat Luxemburg eine Entschädigung von 15.000 Euro und 40.000 Euro Prozesskosten erhält (Az. No. 21884/18). Halet war an den Enthüllungen der „Lux-Leaks-Affäre“ beteiligt und wegen Diebstahls und der Verletzung des Berufsgeheimnisses zu einer vermeintlich geringen Geldstrafe von rund 1.000 Euro verurteilt worden. Aber Strafe bleibt Strafe, so sein Anwalt. Auch das würde Whistleblower abschrecken.

In der „Lux-Leaks-Affäre“ waren vertrauliche Steuervereinbarungen zwischen Luxemburg und 340 multinationalen Konzernen öffentlich geworden. Zu den Unternehmen, die infolge der Vereinbarungen die Möglichkeit bekamen Milliarden Dollar an Steuern zu vermeiden, gehörten Amazon, Apple, Ikea, Pepsi, AIG und Verizon. Geschlossen wurden die Vereinbarungen unter dem damaligen luxemburgischen Ministerpräsidenten und späteren EU-Kommissionschef Jean-Claude Juncker.

Kläger Halet freute sich nach elf Jahren endlich Recht zu bekommen: „Es geht hier nicht um mich, es geht um unsere Kinder, um andere Whistleblower, um andere Bürger, die sich jetzt auf diese Argumente berufen können.“ Nach all den guten und schlechten Phasen, die er durchlebt habe, könnten sich andere zukünftig auf das Urteil stützen, wenn es um die Verurteilung von Whistleblowern gehe.

Bislang hatte Halet immer vor Gericht verloren. Der frühere Mitarbeiter von PricewaterhouseCoopers (PwC) wurde verurteilt, weil er die Interessen seines Arbeitgebers verletzt hätte. Er könne sich nicht darauf berufen, dass er im Interesse der Öffentlichkeit gehandelt habe, denn seine Informationen seien ja so neu nicht gewesen. Tatsächlich war Halet nur der zweite Whistleblower in der Offenlegung der Lux-Leaks.

Zunächst hatte ein anderer Mitarbeiter von PwC, Antoine Deltour, 45.000 Seiten Kopien von internen Dokumen-

ten an einen Journalisten weitergegeben. Erst als die Presse auf dieser Grundlage berichtete, dass der Luxemburger Staat durch Vermittlung von PwC in großem Stil internationale Konzerne von der Steuer befreite, meldete sich Halet mit weiteren tausenden Dokumenten 2012 bei der Presse. Weltweit berichteten daraufhin Medien Ende 2014 in den Lux-Leaks über die zweifelhaften Steuerabsprachen von Konzernen mit Luxemburgs Finanzbehörde. Die Veröffentlichungen trugen dazu bei, dass in der Europäischen Union Steuertricksereien erschwert wurden. Weil es nichts Neues gewesen sei, wurde Halet verurteilt.

Für Halets Anwalt war dieser Umstand ein unzulässiges Argument: „Es ist Sache des jeweiligen Journalisten seine Quellen zu bewerten. Das ist nicht die Aufgabe der Quelle selbst. Das darf man den Whistleblowern nicht zur Last legen." Das sahen die Richterinnen und Richter des EGMR in Straßburg genauso. Das öffentliche Interesse, solche Vorgänge aufzudecken, sei deutlich gewichtiger gewesen als das Interesse des Arbeitgebers vertrauliche Informationen nicht nach außen getragen zu bekommen. Halet habe in jedem Fall zu einer öffentlichen Debatte beigetragen und sei in seiner Meinungsfreiheit verletzt. Die Luxemburger Gerichte hätten den Fall also nicht richtig beurteilt. Auch geringe Strafen hätten einen abschreckenden Effekt auf alle, die im Sinne der Öffentlichkeit etwas offenlegen wollen. Ein solcher Eingriff in die Meinungsfreiheit sei in einer demokratischen Gesellschaft nicht notwendig.

Das Urteil aus Straßburg ist bemerkenswert, da der Gerichtshof in einem ersten Durchgang Halet eine Abfuhr erteilt hatte. Im Mai 2021 hatte das Gericht befunden, dass die vom belgischen Gerichtshof verhängte Strafe nachvollziehbar sei. Dies revidierte nun die Große Kammer. Sie hält dabei an den Kriterien fest, nach denen sie seit einem Grundsatzurteil von 2008 zwischen den Belangen der Unternehmen und dem Schutz der Hinweisgeber abwägt. Doch hat der Gerichtshof die Gewichte anders verteilt. Das Urteil war umstritten; fünf Mitglieder der Kammer formulierten abweichende Meinungen (Deppe, Informant Halet zu Unrecht bestraft, www.tagesschau.de 14.02.2023; „Lux Leaks": EGMR gibt Whistleblower recht, 14.02.2023, https://orf.at/stories/3305197/; Janisch, Schutz für Whistleblower, SZ 15.02.2023, 21).

EuGH

Interessenkonflikte rechtfertigen Abberufung als Datenschutzbeauftragter

Der Europäische Gerichtshof (EuGH) entschied mit Urteil vom 09.02.2023, dass ein betrieblicher Datenschutzbeauftragter seine Aufgabe neutral erfüllen können muss, was bei einem Interessenkonflikt nicht der Fall ist (Az. C-453/21 u. C-560/21). Die Anforderungen des Bundesdatenschutzgesetzes (BDSG) zur Abberufung eines Datenschutzbeauftragten stehen denen der EU-Datenschutz-Grundverordnung (DSGVO) nicht entgegen. Ob die Voraussetzungen für die Abberufung vorliegen, muss das Gericht im Einzelfall überprüfen. Ein solcher Interessenkonflikt besteht, wenn der Arbeitnehmer in einem Unternehmen gleichzeitig vom Arbeitgeber damit betraut wird personenbezogene Daten, etwa von Kunden, zu verarbeiten oder wenn dieser selbst den Zweck der Datenverarbeitung festlegt. Dies kann nach EU-Recht die Abberufung als Datenschutzbeauftragter erforderlich machen.

Gemäß der DSGVO darf ein betrieblicher Datenschutzbeauftragter nicht abberufen werden, nur weil er seine Aufgaben erfüllt. Deutsches Recht sieht für die Abberufung noch strengere Voraussetzungen vor. Danach ist diese nur „aus wichtigem Grund" erlaubt. Das Bundesarbeitsgericht (BAG) hatte hierzu zwei Verfahren dem EuGH zur Prüfung vorgelegt. Im ersten Fall ging es um einen Betriebsratsvorsitzenden des Halbleiterherstellers X-Fab in Dresden, der gleichzeitig Datenschutzbeauftragter des Unternehmens war. Der Arbeitgeber meinte, dass der Mann als Betriebsratsvorsitzender nicht unabhängig seine Datenschutztätigkeiten ausüben könne und berief ihn von seinem Amt als Datenschutzbeauftragter ab. Im zweiten Fall hatte der Kommunale Zweckverband für Informationsverarbeitung Sachsen (KISA) seinen Datenschutzbeauftragten abberufen. Dieser sei in seiner beruflichen Tätigkeit mit der Verarbeitung personenbezogener Daten befasst.

Dr. Christoph Ceelen, unternehmensnaher Fachanwalt für Arbeitsrecht bei der internationalen Wirtschaftskanzlei CMS Deutschland, erklärte dazu: „Das Urteil ergänzt die bisherige Rechtsprechung des EuGH zur starken Rechtsstellung eines Datenschutzbeauftragten. Bereits 2022 hielt der EuGH den deutschen Sonderkündigungsschutz des Beauftragten für vereinbar mit dem Unionsrecht. Damit ist klargestellt, dass interne Datenschutzbeauftragte umfassenden Bestandsschutz genießen." Mit Blick auf die praktische Bedeutung meinte er allerdings, „das Urteil bringt Arbeitgebern keine Klarheit. Ob die Voraussetzungen einer Abberufung vorliegen, lässt der EuGH nationale Gerichte im Einzelfall prüfen. Insofern ist zu befürchten, dass sich die Zwickmühle für Arbeitgeber nicht ändert: Im entschiedenen Fall hatte eine Behörde die Abberufung des Betriebsratsvorsitzenden wegen des befürchteten Interessenkonflikts gefordert. Vor den Arbeitsgerichten war der Arbeitgeber mit der Abberufung aber gescheitert – Arbeitsgerichte verneinen seit längerem den Interessenkonflikt zwischen beiden Ämtern." Mit der bestätigten, starken Stellung interner Datenschutzbeauftragter sollten Unternehmen gut abwägen, ob sie eine externe Vergabe des Amts vorziehen, meint Ceelen. Die Abberufungsgründe, die der EuGH aufführt, werde ein Arbeitgeber selten nachweisen können (Urteil zu Interessenkonflikten von Datenschutzbeauftragten in Firmen, Tagesspiegel Background, Digitalisierung & KI, 10.02.2023; Abberufung von Datenschutzbeauftragten aus wichtigem Grund möglich, www.lto.de 09.02.2023).

BVerfG

Polizeiliche komplexe Datenanalyse nur unter engen Voraussetzungen

Das Bundesverfassungsgericht (BVerfG) hat mit Urteil vom 16.02.2023 den Einsatz automatisierter Daten-

analysen durch die Polizei gemäß den Gesetzen von Hessen und Hamburg für verfassungswidrig erklärt, weil diese Gesetze weder Art und Menge der Daten noch die technischen Methoden bis hin zu Künstlicher Intelligenz (KI) und Profiling hinreichend eingeschränkt regeln und deshalb Persönlichkeits- und Vertraulichkeitsrechte des Grundgesetzes verletzen (1 BvR 1547/19 u. 1 BvR 2634/20).

• Data-Mining: nützlich und gefährlich

Das BVerfG stellte zum Data Mining bei der Polizei fest, dass automatisierte Datenanalysen durch die Polizei durchaus ein geeignetes und auch erforderliches Mittel sein können in Zeiten „von ständig anwachsenden und nach Qualität und Format zunehmend heterogenen Datenaufkommen." Die beiden angegriffenen Regelungen (§ 25a Abs. 1 Alt. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und § 49 Abs. 1 Alt. 1 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei) erlaubten dagegen praktisch eine „automatisierte Verarbeitung unbegrenzter Datenbestände mittels rechtlich nicht eingegrenzter Methoden". Die beiden Landesgesetzgeber haben damit gemäß dem Urteil den Grundsatz der Verhältnismäßigkeit massiv verletzt. Berichterstatterin war die Richterin Gabriele Britz.

Notwendig für die besonders eingriffsintensiven Maßnahmen sind klare Eingriffsschwellen und die Eingrenzung auf besondere Fälle. Nur wenn sehr eingegrenzte Datensätze und einfachere Methoden zum Einsatz kommen, könne die Eingriffsschwelle niedriger angesetzt werden. Die erfolgenden Zweckabänderungen gegenüber der ursprünglichen Zweckbindung der Daten sind an bestimmte Anforderungen zu knüpfen.

Automatisierte Datenanalysen oder Datenauswertungen verursachen gemäß dem Grundsatzurteil besondere Belastungseffekte, „die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen." Über die Verarbeitung großer und komplexer Datenbestände mit praktisch allen informationstechnisch möglichen Methoden könnten weitreichende Erkenntnisse abgeschöpft werden. Ebenso könnten aus der Auswertung neue Zusammenhänge erschlossen werden. Bei entsprechendem Einsatz komme der Einsatz der in Frage stehenden Polizeitools einem „Profiling" nahe. Je mehr durch die Datenanalysen über eine Person in Erfahrung gebracht werden kann und je höher die „Fehler- und Diskriminierungsanfälligkeit" ist, desto gravierender sind die Analysen. Auch die Nachvollziehbarkeit softwaregestützter Verknüpfungen fällt nach Ansicht der Richter ins Gewicht.

• Gesetze gekippt

Beteuerungen, dass aktuell eine unbegrenzte Datenauswertung technisch noch gar nicht möglich sei, retteten die einmal mehr vor dem Verfassungsgericht gescheiterten Landesgesetzgeber nicht: „Selbst wenn Funktionsweiterungen erst infolge weiterer technischer Entwicklungen möglich sind, richten sich die verfassungsrechtlichen Anforderungen grundsätzlich nach den rechtlich schon jetzt geschaffenen Eingriffsmöglichkeiten." Der Versuch der Vertreter aus Hamburg durch Verwendung des Wortes „Datenauswertung" anstelle des Wortes „Datenanalyse" zu weitgehende Anwendungen auszuschließen, war verfassungsrechtlich nicht ausreichend, so der Vorsitzende Richter Stephan Harbarth.

Das Gericht kippte Hamburgs bislang noch nicht zum Einsatz gekommene Regel mit sofortiger Wirkung. Für Hessen-Data, das angeblich noch keine selbstlernenden Analysen nutzt und laut dem Richterspruch bereits tausendfach eingesetzt wird, gaben sie noch eine Gnadenfrist bis 30.09.2023. Bis dahin müssen die Landesgesetzgeber die fein ziselierten Differenzierungen zu Eingriffstiefen ihrer Analyse-Software und den abzudeckenden Tatbeständen neu fassen. Gemäß Hessens Innenminister Peter Beuth bei der Verhandlung wurde mit dem neuen Verfahren erfolgreich eine Serie von Geldautomatensprengungen aufgeklärt: „Manchmal sind es die kleinsten Teile, die die größte Erkenntnis bringen." So konzedierte auch Harbarth, dass die automatisierte Analyse „relevante Erkenntnis" zutage fördern könne. Das Urteil sei kein Veto gegen den Einsatz moderner Technologie. Dieser müsse aber rechtsstaatlich flankiert sein.

• Hohe Schwelle für KI-Einsatz

Beuths Diktum vom Nutzen der vielen kleinen Dinge hat Schattenseiten, die das Urteil deutlich macht, nämlich große Risiken für die Grundrechte. Das „neue Wissen" ist fehleranfällig. Gemäß dem Gericht greift der Einsatz lernfähiger KI-Systeme besonders tief in die Grundrechte ein, weil es sich von der kriminologisch fundierten Programmierung löst und seine Suchmuster weiterentwickelt. Solche Systeme könnten „selbständig weitere Aussagen im Sinne eines ‚predictive policing'" treffen. Sie emanzipieren sich also von ihren polizeilichen Urhebern und durchlaufen maschinelle Lernprozesse, die keiner mehr durchschaut. Diese Stärke der KI ist zugleich wegen des Black-Box-Phänomens eine Gefahr, wenn der Staat auf dieser Basis gegen Betroffene mit Gewalt vorgeht: „Dann droht zugleich die staatliche Kontrolle über die Anwendung verloren zu gehen."

Das BVerfG spricht eine weitere Schwäche von KI an: ihre Anfälligkeit für Diskriminierung. Das ist meist ein Problem der Trainingsdaten. Wenn das System lernt, dass Tatverdächtige häufig aus bestimmten Ländern stammen, dann reproduziert es diese Erkenntnisse und vertieft sie, obwohl der Umstand, dass Ausländer häufiger verdächtigt werden, meist Konsequenz menschlicher Vorurteile ist. Das Gericht mahnt deshalb KI mit spitzen Fingern anzufassen: „Daher dürfen selbstlernende Systeme nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz eingeschränkter Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern."

Das Urteil liefert eine Ansammlung von Schwellen und Hürden, die überwunden werden müssen, bevor automatisierte Datenanalyse zum Einsatz kommt. Die Höhe der Schwelle hängt davon ab, wie intim oder wie umfassend die Daten sind, die in den großen Topf geworfen werden. Das von Hessen z.B. genutzte Vorgangsbearbeitungssystem ComVor ist ein riesiger Datenbestand, in dem auch Lappalien wie z.B. Fundsachen gespeichert sind. Der gekippte Pa-

ragraf hätte der Polizei sogar die Lizenz zur Facebook-Recherche verschafft. Die Schwelle für den Einsatz von KI ist ähnlich hoch wie bei Lauschangriff oder Online-Durchsuchung. Es muss um den „Schutz besonders gewichtiger Rechtsgüter gehen“, also um eine „hinreichend konkretisierte Gefahr“ für Leib, Leben oder Freiheit der Person.

• Praktische Folgen für VeRA

Bijan Moini, Leiter des Legal Teams der Gesellschaft für Freiheitsrechte (GFF), begrüßte das Urteil: „Die Klage der Gesellschaft für Freiheitsrechte hat das Risiko deutlich reduziert, dass unbescholtene Bürgerinnen und Bürger ins Visier der Polizei geraten. Unsere strategische Prozessführung wirkt.“ Die GFF hatte zusammen mit der Humanistischen Union und weiteren Organisationen und Einzelpersonen geklagt. Das Urteil ist nach Ansicht der Beschwerdeführer ein wichtiger Meilenstein; die Debatte um die Automatisierung der Polizeiarbeit habe gerade erst begonnen.

Für das Bayerische Innenministerium ist das Urteil von besonderer Relevanz, da dessen Polizei 2022 die Software Gotham des US-Anbieters Palantir für das geplante Projekt VeRA (Verfahrensübergreifende Recherche- und Analyseplattform) als Musterverfahren ausgewählt hat (DANA 2/2022, 106). Im Januar 2023 hatte Bayerns Innenminister Joachim Herrmann angekündigt, man werde erst nach dem Karlsruher Urteil eine Rechtsgrundlage im Bayerischen Polizeigesetz für den Gotham-Einsatz schaffen. Während die vorangegangenen Polizeiaufgabengesetze aus Bayern noch auf den Tischen der Verfassungsrichter in München und Karlsruhe liegen, will man sich dieses Mal besser absichern. Für das um die Datenanalysen erweiterte PAG 3.0 hat man nicht zuletzt auf Drängen der Opposition in Bayern für 430.000 Euro eine Studie beim Fraunhofer Institut SIT in Auftrag gegeben. Die soll das Risiko von Datenabflüssen aus dem auf Gotham basierenden VeRA abschätzen. Die Studie ist laut Innenminister Herrmann fertig und wurde im Februar dem zuständigen Ausschuss im Bayerischen Landtag vorgestellt. Dann, so Herrmann, könne auch hier der Gesetzgebungsprozess starten. Das Bundesland Nordrhein-Westfalen setzt die Dienste von Palantir bereits ein.

Das bayerische Ausschreibungsverfahren ist bedeutsam, weil dabei ein Rahmenvertrag für den Einsatz der Gotham-Analysetools für die Polizeibehörden der Länder und des Bundes ausgehandelt wurde. Damit würde Palantir zu einem fast schon monopolartigen Anbieter für die Datenanalysen in Deutschland, und auch in Europa ist der Anbieter gut im Geschäft. Das Projekt dieser Datenauswertung wurde 2022 mit einem BigBrotherAward prämiert (DANA 2/2022, 92). Zur Kundschaft gehört auch Europol, dessen neue Big-Data-Praxis aktuell der Europäische Beauftragte für Datenschutz (EDPS) vom Europäischen Gerichtshof (EuGH) prüfen lässt. Denn Europol hatte sich die vom EDPS gerügte Praxis, große Datensätze der Mitgliedsstaaten zum Zwecke von Analysen längerfristig zu speichern, durch eine neue Verordnung absegnen lassen die rückwirkend die nicht Datenschutz-konforme Praxis zu legalisieren versucht (DANA 2/2022, 110, 4/2022, 265 f.). Das nun gefällte Urteil des BVerfG kann hier für den EuGH stilbildend sein (Ermert, Bundesverfassungsgericht beanstandet Regeln zur Datenanalyse bei der Polizei, www.heise.de 16.02.2023; Kurzlink: https://heise.de/-7517629; Janisch, Künstliche Intelligenz, die zu weit geht, SZ 17.02.2023, 6; siehe auch den Beitrag von Mannah, S. 93).

BVerfG

Vor allem verdeckte Polizeibefugnisse in Mecklenburg-Vorpommern sind verfassungswidrig

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 09.12.2022 mehrere Vorschriften zu polizeilichen Ermittlungsbefugnissen in Mecklenburg-Vorpommern (Sicherheits- und Ordnungsgesetz – SOG MV) wegen Verstoß gegen das Recht auf informationelle Selbstbestimmung, den Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, das Fernmeldegeheimnis sowie die Unverletzlichkeit der Wohnung für verfassungswidrig erklärt (1 BvR 1345/21). Die Klage hatte die Gesellschaft für Freiheitsrechte (GFF) zusammen mit dem Bündnis „Sogenannte Sicherheit“ im Juni 2021 eingereicht, um sich gegen die Überwachung von Menschen ohne konkreten Anlass zu stellen. Laut GFF handelt es sich bei der Entscheidung der Karlsruher Richter um ein Grundsatzurteil, das auch für andere Bundesländer Grenzen für die Verschärfung von Polizeigesetzen setzt.

Neben der nun entschiedenen Verfassungsbeschwerde laufen zu weiteren Bundesländern Klagen gegen die Verschärfung der dortigen Polizeigesetze. 2019 hat die GFF zudem Beschwerde gegen ein 2017 reformiertes Bundeskriminalamtsgesetz (BKAG) eingelegt, um sich gegen verdeckte Überwachungsmaßnahmen wie Staatstrojaner zu stellen. Es wird kritisiert, dass mit diesem Gesetz große Datenbanken über viele Menschen in Deutschland zeitlich unbegrenzt und „nach unklaren Regeln und zu unklaren Zwecken“ angelegt werden könnten. Zuvor hatte 2016 das Bundesverfassungsgericht wesentliche Teile des BKA-Gesetzes für verfassungswidrig erklärt (BVerfG 20.04.2016 – 1 BvR 1140/09), das aber nach Ansicht der GFF unzureichend novelliert worden ist.

Das Land Mecklenburg-Vorpommern hatte im Lichte dieses Urteils 2020 das SOG MV novelliert und neben anlasslosen Abhörmaßnahmen in und außerhalb der Wohnung den heimlichen Einsatz von Staatstrojanern und der Rasterfahndung ohne konkrete Gefahr auch eine längerfristige Überwachung ohne Anlass durch Polizeibeamte ermöglicht. Ebenfalls erlaubt wurde damit das heimliche Betreten der Wohnung zwecks PC-Durchsuchung oder Quellen-Kommunikationsüberwachung (Quellen-TKÜ). Damit wäre auch die Überwachung der Messenger-Kommunikation vor oder nach deren Entschlüsselung möglich. Die Behörden greifen dafür meist auf sogenannte Staatstrojaner zurück.

Das BVerfG beanstandete eine Regelung, die sich mit dem Einsatz von Vertrauenspersonen (V-Leuten) und verdeckt Ermittelnden befasst, weil sie den „Kernbereich privater Lebensgestaltung“ nicht ausreichend schützt. So wird vom Gericht der rechtlich nahezu unantastbare Bereich des menschlichen

Daseins beschrieben. Die Vorschrift hat zwar im Blick, dass Leute im Undercover-Einsatz sich sehr nahe an ihre „Zielperson“ heranmachen müssen. Davon machte das Gesetz aber allzu großzügige Ausnahmen. Schon eine nicht näher beschriebene „Gefährdung“ von Polizisten oder V-Leuten sollte genügen, damit sie weiter ermitteln dürfen. Das Gericht kippte die Vorschrift und stellt zum delikaten Thema des Sexeinsatzes – bekannt als Romeo- oder Venusfalle – klar, dass hier in die privateste Sphäre eingedrungen wird, „weil staatlich veranlasst privateste Beziehungen auf täuschungsbedingter Grundlage entstünden“. Hierdurch kann sich der Staat Zugang zu besonders intimen Informationen verschaffen, was in jedem Fall verfassungswidrig ist: „Ausgeschlossen wären etwa staatlich veranlasstes Eingehen einer intimen Beziehung zum Zweck der Informationsgewinnung oder der Einsatz einer Person als Vertrauensperson gegenüber der eigenen Ehepartnerin oder dem eigenen Ehepartner.“

Die Entscheidung beanstandet zudem weitere verfassungsrechtliche Grenzüberschreitungen. Immerwährendes Thema von Polizeigesetzen ist die Frage, bei welchem Gefahrengrad die Polizei zu welchen Überwachungsmaßnahmen greifen darf. Inzwischen existiert insofern eine feine Abstufung, die von einer „wenigstens konkretisierten Gefahr“ bis zur „dringenden Gefahr“ reicht. Je tiefer der Eingriff in die Grundrechte, desto höher ist die Hürde für die Polizei.

Gemäß dem Urteil verstößt die in § 33b Abs. 1 Satz 2 SOG MV aufgeführte Wohnraumüberwachung gegen das Grundgesetz, „weil die Eingriffsschwelle nicht dem Erfordernis einer dringenden Gefahr“ genügt. David Werdermann, Jurist und Verfahrenskoordinator, erläutert: „Tiefe Grundrechtseingriffe wie die Wohnraumüberwachung oder die Telekommunikationsüberwachung sind nur gerechtfertigt, wenn eine konkrete Gefahr vorliegt. Die Polizeirechtsverschärfungen in verschiedenen Bundesländern, die Überwachung weit im Vorfeld einer Gefahr zulassen, verletzen das Grundgesetz.“ „Sogenannte Sicherheit“-Sprecher Micha Milz ergänzt: „Hier wird besonders deutlich, dass die Landesregierung unter dem Vorwand der Terrorbekämpfung massenweise Daten verarbeiten wollte, ohne dass eine konkrete Gefahr vorliegen musste.“ Beanstandet wurde auch die Regelung zur Online-Durchsuchung (§ 33c Abs. 1 Satz 2 SOG MV).

Das SOG MV bediente sich an mehreren Stellen eines gern verwendeten Kunstgriffs: Es verweist auf sog. Vorfeldparagrafen im Strafgesetzbuch, die ihrerseits bestimmte Gefahrenlagen unter Strafe stellen. Dazu gehört u.a. die „Vorbereitung einer schweren staatsgefährdenden Gewalttat“. Täter können mit bis zu zehn Jahren Haft bestraft werden, weil sie die Gefahr eines Anschlags geschaffen haben. Kombiniert man solche Vorschriften mit dem Polizeigesetz, entsteht eine Art Verdoppelungseffekt: Die Polizei dürfte etwa einen Lauschangriff schon schalten, wenn die Gefahr einer Gefahr besteht. Das wird vom BVerfG nicht hingenommen: Durch solche Verknüpfungen werde „die Eingriffsschwelle in verfassungswidriger Weise abgesenkt“.

Ein Teil der verfassungswidrigen Vorschriften wurde nicht aufgehoben, sondern lediglich für mit der Verfassung unvereinbar erklärt – verbunden mit der Anordnung ihrer befristeten Fortgeltung. Grund dafür ist, dass nicht der Kern der mit ihnen eingeräumten Befugnisse betroffen ist, sondern einzelne Aspekte ihrer rechtsstaatlichen Ausgestaltung, die der Gesetzgeber bis Ende 2023 nachbessern kann, damit die verfolgten Ziele auf verfassungsmäßige Weise verwirklicht werden können.

Über manche Punkte wurde aus formellen Gründen nicht entschieden, etwa über Drohneneinsätze, da nicht klar war, inwieweit dies die Beschwerdeführer betrifft. Rechtsanwältin Kathrin Hildebrandt aus Rostock, eine der Beschwerdeführerinnen, betont: „Nach dem Gesetz wären (...) nicht nur viele meiner Mandanten, sondern auch ich selbst als deren sogenannte Kontaktperson, Maßnahmen wie längerfristigen Observationen, Kamera-Überwachung oder der Ausspähung durch verdeckte arbeitende Polizeibeamte oder mit der Polizei zusammenarbeitende Personen ausgesetzt.“ Das Polizeigesetz muss also umfassend überarbeitet werden (Koch, www.heise.de 01.02.2023; Kurzlink: https://heise.de/-7477964; Janisch, Ende des Polizei-Romeos, SZ 02.02.2023, 5; BVerfG, PM 15/2023 v. 01.02.2023, Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern teilweise verfassungswidrig).

BVerwG

Handyauslesen bei Asylsuchenden nur im Ausnahmefall

Das Bundesverwaltungsgericht (BVerwG) hat mit Urteil vom 16.02.2023 entschieden, dass der Ansatz des Bundesamts für Migration und Flüchtlinge (BAMF), Handys und andere Datenträger bei der Registrierung von Asylantragstellern zu durchsuchen und auszuwerten, wenn diese keine Pässe oder Ersatzpapiere vorweisen können, unrechtmäßig ist (Az. 1 C 19.21). Es gab einer klagenden Afghanin recht, die im Jahr 2019 ins Bundesgebiet einreiste und mit einem nationalen Ausweisdokument (Tazkira) ohne biometrische Daten und mit Heiratsurkunde Asyl beantragte.

Das BAMF forderte die Klägerin damals auf ihr Mobiltelefon herauszugeben sowie dessen Zugangsdaten mitzuteilen. Dem kam die Asylbewerberin nach, die ihr Handy nach der Datenauslesung und -speicherung zurückbekam. Dagegen wehrte sich die Frau im Frühjahr 2020 gerichtlich mit Unterstützung der Gesellschaft für Freiheitsrechte (GFF), die noch weitere verwaltungsgerichtliche Klagen in ähnlich gelagerten Fällen koordiniert. Laut der Bürgerrechtsorganisation ist die Analyse von Daten aus portablen Datenträgern von Asylantragstellern durch BAMF ein unverhältnismäßig tiefer Eingriff in die Privatsphäre und zudem fehleranfällig.

Das Verwaltungsgericht hatte festgestellt, dass die Anordnung gegenüber der Klägerin, die Zugangsdaten für ihr Mobiltelefon zur Verfügung zu stellen, rechtswidrig und das Bundesamt nicht berechtigt gewesen sei die Daten der Klägerin von ihrem Mobiltelefon auszulesen, mittels Software auszuwerten, den aus der Auswertung generierten Ergebnisreport für das Asylverfahren freizugeben und der Entscheidung über den Asylantrag zugrunde zu legen. Die sonst vorliegenden Erkenntnisse und

Dokumente hätten gegenüber der Datenauswertung ein milderes Mittel zur Identitätsfeststellung dargestellt.

Das BVerwG bestätigte mit dem Urteil nun die Entscheidung der Vorinstanz und wies die dagegen gerichtete Revision des BAMF zurück. Die Auswertung von Mobiltelefonen und anderen Datenträgern sei erst zulässig, wenn die Identitätsfeststellung „nicht durch mildere Mittel erreicht werden kann" (§ 15a Abs. 1 Satz 1 AsylG). Im konkreten Fall hätte das BAMF etwa noch Tazkira und Heiratsurkunde heranziehen sowie Registerabgleiche und Nachfragen beim Sprachmittler zu sprachlichen Auffälligkeiten durchführen können. Das Vorgehen der Behörde war daher unverhältnismäßig.

Das BAMF darf Handy-Daten prinzipiell seit einer umstrittenen Reform des Asylgesetzes im Jahr 2017 auswerten, um die Ausreisepflicht besser durchzusetzen. Mitarbeiter können auf dieser Basis auch Laptops, Tablets und USB-Sticks von Asylbewerbern ohne richterliche Genehmigung auslesen, um deren Identität und Staatsangehörigkeit festzustellen. Die Regel greift aber nur, wenn ein Migrant Name und Herkunft nicht anderweitig nachweisen kann. Für die GFF-Verfahrenskoordinatorin Lea Beckmann ist das Urteil ein „großer Erfolg". Das BAMF müsse seine Praxis jetzt prinzipiell stoppen. Die GFF ist überzeugt, dass das Auslesen von Handys und die Auswertung der Daten nicht mit der Datenschutz-Grundverordnung (DSGVO) und der EU-Grundrechtecharta vereinbar ist. Beim Bundesdatenschutzbeauftragten Ulrich Kelber ist dazu noch eine Beschwerde anhängig.

Dessen Vorgängerin Andrea Voßhoff hatte die Befugnis während des Gesetzgebungsverfahrens als potenziell verfassungswidrig eingestuft. Kelber bestätigte: „Seit vielen Jahren schaffen die Gesetzgeber in EU, Bund und Ländern immer neue Möglichkeiten für die Datenerhebung von Behörden, die sich danach als rechtswidrig herausstellen." Das müsse sich dringend ändern; die Bürger verlören ansonsten das Vertrauen in die Politik (Bundesverwaltungsgericht, PM Nr. 13/2023 v. 16.02.2023, Voraussetzungen der Auswertung digitaler Datenträger durch das Bundesamt für Migration und Flüchtlinge im Asylverfahren; Krempl, Gängige Praxis zur Handy-Datendurchsuchung bei Flüchtlingen ist rechtswidrig, www.heise.de 17.02.2023, Kurzlink: https://heise.de/-7519706).

VG Hannover

Handscanner-Leistungskontrolle bei Amazon ist verhältnismäßig

Gemäß einem Urteil des Verwaltungsgerichts (VG) Hannover vom 09.02.2023 darf Amazon in seinem Logistikzentrum in Winsen (Luhe) bei Hamburg weiterhin und unverändert die Arbeitsgeschwindigkeit der Mitarbeiter mithilfe von Handscannern überwachen (Az. 10 A 6199/20). Das Verfahren fand vor Ort bei Amazon in Winsen statt; die Richterinnen und Richter hatten sich auch von Amazon durch das Logistikzentrum führen lassen. Mit dem Urteil erklärte das VG eine Verfügung der niedersächsischen Datenschutzbehörde, der Landesbeauftragten für Datenschutz, für rechtswidrig. Die Behörde hatte Amazon die „ununterbrochene jeweils aktuelle und minutengenaue Erhebung und Verwendung bestimmter Beschäftigtendaten" untersagt. Dagegen wehrte Amazon sich mit der Klage vor dem VG.

Die entscheidende Frage war die nach der Verhältnismäßigkeit: Was wiegt schwerer – das Interesse Amazons, die Abläufe im Logistikzentrum zu optimieren und die Leistung der Mitarbeiter zu überwachen, oder der Schutz der Menschen vor der Erfassung jedweden Arbeitsschritts? Die Vorsitzende der Kammer erklärte, die Abwägung sei „sehr schwierig" gewesen: „Wir haben keine Zweifel, dass es einen Anpassungs- und Überwachungsdruck gibt." Dies gelte besonders für die befristet Beschäftigten. Doch die Interessen Amazons seien gewichtiger.

Das Gericht führte unter anderem an, dass die Überwachung auch positiv auf die Mitarbeiter wirke, da sie objektives Feedback ermögliche. Sie reduziere zudem Stress, da Mitarbeiter „gemäß ihres Könnens" eingesetzt werden könnten: „Das führt zu gleichmäßigerer Lastenverteilung und geringerer Frustration." Es gehe außerdem nicht um besonders sensible Daten oder eine Verhaltenskontrolle, sondern nur um die Leistung. Obendrein habe das Gericht den Eindruck gewonnen, dass dem Betriebsrat „wegen der Überwachung nicht die Bude eingerannt wird". Aus Sicht der Richter ist die Verfügung der Datenschutzbehörde noch aus einem weiteren Grund rechtswidrig: Sie sei gar nicht geeignet die Rechte der Mitarbeiter zu schützen. Da die Behörde bloß „ununterbrochene" Datenerfassung untersagt habe, könne Amazon den Prozess für eine Minute oder Sekunde unterbrechen und sogleich fortsetzen, womit den Mitarbeitern aber nicht geholfen wäre.

Zur „Beweisaufnahme" befragte das Gericht auch eine ehemalige sowie den aktuellen Betriebsratsvorsitzenden. Dabei kam unter anderem zur Sprache, dass Amazon die per Handscanner erfassten Daten zur Arbeitsgeschwindigkeit nicht nur für Personalentscheidungen und spontane „Feedbackgespräche" verwendet, sondern dass die Mitarbeiter an bestimmten Stationen ihren aktuellen Geschwindigkeitswert auch ständig angezeigt bekommen. Grundsätzlich erfassen die Mitarbeiter mit den Handscannern, welches Produkt sie in welchen Transportkorb oder welches Regalfach gelegt haben. Amazon nutzt diese Daten nicht nur zur Qualitätssicherung und zur Vermeidung von Warenstaus im Logistikzentrum, sondern verknüpft sie auch mit den Profilen der Mitarbeiter.

Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen, Barbara Thiel, kommentierte die Entscheidung: „Ich bin nach wie vor der Auffassung, dass das allgemeine Persönlichkeitsrecht der Mitarbeiterinnen und Mitarbeiter überwiegt. Der durch die minutengenaue Leistungsdatenerhebung sowie deren weitere Verarbeitung entstehende Anpassungs- und Leistungsdruck ist aus meiner Sicht höher zu gewichten als das wirtschaftliche Interesse des Unternehmens." Wie das VG sieht auch die LfD, dass für den Beschäftigtendatenschutz dringender Handlungsbedarf des Bundesgesetzgebers besteht und klare Regelungen erlassen werden müssen: „Die Grenzen einer Datenverarbeitung von Beschäftigten müssen gesetzlich klar festgelegt werden." Ein Sprecher der Datenschutzbehörde ergänzte, die Tatsache, dass das Gericht eine Beru-

fung zugelassen habe, sei ein Hinweis darauf, dass auch eine andere Sichtweise nicht als abwegig angesehen werde. Die Behörde legte Berufung ein. Ein Vertreter von Amazon erklärte: „Wir freuen uns über die Entscheidung des Verwaltungsgerichts Hannover." Warenwirtschaftssysteme seien branchenüblich und Untersuchungen zeigten, dass sie sich positiv auf die Arbeitserfahrung der Mitarbeiter auswirken (Wölbert, Leistungsüberwachung: Amazon gewinnt vor Gericht gegen Datenschutzbehörde, www.heise.de 09.02.2023, Kurzlink: https://heise.de/-7491037; Thiel: „Das allgemeine Persönlichkeitsrecht der Mitarbeiterinnen und Mitarbeiter überwiegt unternehmerische Interessen", PE LfD Nds. 10.02.2023).

VG Hamburg

Einstweilige Anordnung gegen Fingerabdruck auf Personalausweis

Das Verwaltungsgericht (VG) Hamburg ordnete mit Beschluss vom 22.02.2023 an, dass einer Privatperson einstweilig ein Personalausweis ohne darauf gespeicherte Fingerabdrücke ausgestellt werden muss (Az.: 20 E 377/23). Seit August 2021 sind Bundesbürger beim Beantragen eines neuen Personalausweises gesetzlich verpflichtet mit einem Scanner Abdrücke des linken und rechten Zeigefingers abnehmen und auf dem Ausweis digital speichern zu lassen. Das VG Hamburg entschied mit einer einstweiligen Anordnung, dass die zuständige Behörde der Hansestadt einem Antragsteller ein solches hoheitliches Dokument auch ohne die auf dem Chip zusammen mit dem biometrischen Gesichtsbild gespeicherten Fingerabdrücke ausstellen muss. Der Ausweis solle zunächst befristet für ein Jahr gelten, bis die Rechtslage höchstrichterlich geklärt ist.

Die Hamburger Richter bezweifeln in dem Eilverfahren „erheblich" die Rechtmäßigkeit der EU-Verordnung, die die Speicherpflicht für alle Mitgliedsstaaten vorschreibt. Es bestehe Dringlichkeit, um zu vermeiden, dass der Antragsteller „einen schweren und nicht wiedergutzumachenden Schaden erleidet". Ohne Erlass einer einstweiligen Anordnung und die Gewährung vorläufigen Rechtsschutzes wäre dieser gezwungen seine Fingerabdrücke bei der Beantragung eines neuen Personalausweises abzugeben. Dies würde für ihn „einen erheblichen Nachteil bedeuten, da es sich hierbei um besonders geschützte Daten handelt". Die zuständige Behörde kann gegen den Beschluss noch Beschwerde einlegen.

In Deutschland müssen Personen über 16 Jahre einen Personalausweis oder Reisepass besitzen. Sonst drohen Bußgelder bis zu 5.000 Euro. Hintergrund des Hamburger Streits ist eine Klage von Detlev Sieber von der Bürgerrechtsorganisation Digitalcourage vom Dezember 2021 gegen die hiesige Auflage zur Fingerabdruckabnahme und das ihr zugrundeliegende EU-Gesetz vor dem Verwaltungsgericht Wiesbaden, „weil ich nicht wie ein Verbrecher behandelt werden will". Das VG Wiesbaden äußerte Anfang 2022 ebenfalls erhebliche Zweifel an der Rechtmäßigkeit der Bestimmung. Die dortigen Richter hielten sie für unvereinbar mit den Artikeln 7 und 8 der EU-Grundrechtecharta zum Schutz der Privatsphäre (DANA 1/2022, 17). Sie legten den Fall dem Europäischen Gerichtshof (EuGH) vor, der am 14.03.2023 erstmals darüber verhandelte. Das VG Wiesbaden bewertete den Nutzen der biometrischen Chips für vergleichsweise gering, weil der Personalausweis bei der Einreisekontrolle eine weitaus geringere Rolle spiele als der Reisepass, für den der EuGH 2013 die Fingerabdruckpflicht gebilligt hatte.

Die Richter am EuGH fragten bei der Anhörung häufig kritisch nach, insbesondere zur in der Verordnung eingeräumten Frist zwischen der Erhebung der Fingerabdruckdaten in den Behörden und der vorgeschriebenen Löschung. Diese führt dazu, dass die sensiblen biometrischen Merkmale bis zu 90 Tage in den Ämtern gespeichert werden dürfen. Ferner sieht die Verordnung vor, dass die Daten prinzipiell auch für andere Zwecke als die Ausweiserstellung genutzt werden können. Einer der Luxemburger Richter monierte, dass die europäischen Gesetzgeber hier mit dem Ziel, die Sicherheit der Ausweise zu erhöhen, de facto eine neue Sicherheitslücke geschaffen hätten. Insgesamt schien der EuGH die Vorlage aber skeptisch zu sehen. So fragte der als Berichterstatter zuständige Richter Eugene Regan bei der Anhörung, ob biometrische Daten nicht doch ein „angemessener Mechanismus" zur Überprüfung der Identität seien. Die Bürgerrechtler befürchten, dass per Fingerabdruck-Scanner geklaute Scans eine Eintrittskarte zum Identitätsklau und -missbrauch sind. Das Interesse an dem Verfahren ist laut Julia Witte von Digitalcourage hoch: „Wir bekommen unheimlich viele Anfragen von Menschen." Diese lehnten die Speicherpflicht ab und wollten ihre Fingerabdrücke nicht abgeben (Krempl, Verwaltungsgericht: Bürger hat Anspruch auf Personalausweis ohne Fingerabdrücke, www.heise.de 16.03.2023; Kurzlink: https://heise.de/-7547213; Janisch, Hände weg, SZ 15.03.2023, 1).

OLG Frankfurt/Main

„bankrott" als Autocomplete-Voranzeige ist zulässig

Das Oberlandesgericht Frankfurt am Main (OLG) hat mit Urteil vom 20.04.2023 entschieden, dass ein ehemals insolventer Unternehmer keinen Anspruch gegen Google hat, dass bei deren „Autocomplete"-Funktion der Suchmaschine zusammen mit seinem Namen nicht das Wort „bankrott" angezeigt wird (Az. 16 U 10/22). Das OLG meinte, anders als die Vorinstanz des Landgerichts Frankfurt (01.12.2021, Az. 2-34 O 37/21), dass eine solche Verknüpfung in Einzelfällen zulässig sei.

Das Ergebnis der Autocomplete-Funktion sei „erkennbar unbestimmt und enthalte keine eigenständige Behauptung". Der Nutzer wisse, dass es automatisch generiert werde. Konkrete Bedeutung erlange die Kombination erst nach weiteren Recherchen.

Geklagt hatte der Inhaber einer Unternehmensgruppe, die Hotels einrichtet. Zwei Unternehmen dieser Gruppe wurden vor zehn Jahren im Zusammenhang mit Ermittlungen von Steuerbehörden insolvent und sind mittlerweile aus dem Handelsregister gelöscht. Der Kläger wehrte sich dagegen, dass in Googles Suchmaske das Wort „bankrott"

erscheint, sobald sein Vor- und Nachname eingegeben wird. Auch wollte er erreichen, dass eine Webseite, die sich auf die Zahlungsunfähigkeit bezieht, nicht mehr angezeigt und verlinkt wird.

Das OLG meint, der Kläger könne sich mit seiner Forderung nicht auf die Datenschutz-Grundverordnung (DSGVO) berufen. Die Autocomplete-Funktion sei zwar eine automatische Verarbeitung personenbezogener Daten, allerdings müssten hier die Interessen des Klägers auf Achtung des Privat- und Familienlebens, des Schutzes personenbezogener Daten und der unternehmerischen Freiheit zurücktreten. Schwerer wögen das Interesse einer breiten Öffentlichkeit am Zugang zu Informationen sowie Googles Recht auf unternehmerische Freiheit und freie Meinungsäußerung.

Dabei berücksichtigte das OLG, dass die Bedeutung des Suchvorschlags „bankrott" offenbleibe und unbestimmt sei. Einem verständigen Internetnutzer sei bewusst, dass der Suchvorschlag Ergebnis eines automatischen Vorgangs sei. Der Nutzer könne mit der angezeigten Kombination zunächst „nichts anfangen", sie habe keine eigenständige Bedeutung und sei kein Anlass für weitere Recherchen.

Selbst wenn der Nutzer eine Verbindung zwischen dem Kläger und dem Begriff „bankrott" herstellen würde, wäre offen, wie diese Verbindung inhaltlich auszusehen hätte. Zu berücksichtigen sei auch, dass es für die Verbindung zwischen dem Namen des Klägers und dem Begriff „bankrott" tatsächliche Anknüpfungstatsachen gebe. Der Begriff sei auch nicht allein im Sinne von § 283 StGB zu interpretieren, der einen Bankrott unter bestimmten Umständen unter Strafe stellt; er werde vielmehr im allgemeinen Sprachgebrauch verwendet.

Die Entscheidung ist nicht rechtskräftig. Der Kläger kann sich noch an den Bundesgerichtshof (BGH) wenden. Dieser hatte vor fast genau zehn Jahren entschieden, dass Google in seine Suchvorschläge eingreifen muss, wenn sie Persönlichkeitsrechte verletzen. Damals ging es um einen Kläger, der sich durch die automatische Vervollständigung seines Namens um die Begriffe „Scientology" und „Betrug" in seinen Rechten verletzt sah. Gegen Google hatte auch Bettina Wulff, Frau des ehemaligen Bundespräsidenten, geklagt. Sie sah ihren Namen in Googles Suchmaske mit ihr unliebsamen Begriffen verknüpft und einigte sich 2015 mit dem Suchmaschinenanbieter außergerichtlich (Wilkens, Urteil: Googles Autocomplete darf „bankrott" anzeigen, www.heise.de 20.04.2023, Kurzlink: https://heise.de/-8974441; Klage gegen Google zurückgewiesen, https://ordentliche-gerichtsbarkeit.hessen.de 20.04.2023).

LG Ravensburg

Per ED-Maßnahme erzwungener Fingerabdruck dient Handy-Entsperrung

Das Landgericht Ravensburg (LG) hat mit Beschluss vom 14.02.2023 entschieden, dass die Polizei einem Verdächtigen einen Fingerabdruck abnehmen darf, um dessen Mobiltelefon zu entsperren (Az.: 2 Qs 9/23 jug.). Mit dem Auflegen eines Fingers oder dem Blick in die Kamera kann dank biometrischer Mustererkennung ein IT-Gerät wie ein Smartphone oder ein Laptop sekundenschnell ohne Passworteingabe entsperrt werden. Was für den Nutzer bequem ist, macht sich die Justiz zunehmend zunutze. Mit Beschluss des Amtsgerichts Ravensburg vom 12.01.2023 war die aufgrund richterlichen Durchsuchungsbeschlusses bewirkte Beschlagnahme des Mobiltelefons des Beschuldigten bestätigt und die Abnahme und Nutzung der Fingerabdrücke des Beschuldigten zum Zwecke der Entsperrung seines Mobiltelefons angeordnet worden. Die Beschwerde hiergegen blieb erfolglos.

In dem Fall hatte sich ein wegen des Verdachts der Anstiftung zur unerlaubten Einfuhr von und dem Handel mit Betäubungsmitteln in nicht geringer Menge Beschuldigter gegenüber der Polizei geweigert sein Smartphone selbst zu entsperren. Er war insbesondere nicht bereit den passenden Finger auf den Sensor des Handys zu legen. Der Ermittlungsrichter ordnete daraufhin an, dass dem Mann Fingerabdrücke abgenommen werden. Mit damit gefertigten Prints verschafften sich die Beamten Zugang zu dem Mobiltelefon. Der Verdächtige beschwerte sich über das Vorgehen beim Landgericht. Die 2. Strafkammer beschloss daraufhin, dass die angefochtene Entscheidung „der Sach- und Rechtslage" entspreche. Die Anordnung zur Abnahme von Fingerabdrücken des Beschuldigten „auch gegen seinen Willen und erforderlichenfalls im Wege der zwangsweisen Durchsetzung" sowie die Anordnung zur Nutzung der hieraus resultierenden biometrischen Daten für Zwecke der Entsperrung des Mobiltelefons fänden ihre Grundlage in § 81b Abs. 1 Strafprozessordnung (StPO).

In der angeführten Regelung werden erkennungsdienstliche Maßnahmen „für die Zwecke der Durchführung des Strafverfahrens" oder des Erkennungsdienstes erlaubt. Als die Vorschrift in Kraft trat, stand der Abgleich von Fingerabdrücken mit Tatortspuren und Karteikarten oder die Identifizierung von Personen im Vordergrund. Damit soll auch der Aufbau des Europäischen Strafregisterinformationssystems ermöglicht werden. Smartphones und biometrische Erkennungssysteme zur Authentifizierung gab es damals noch nicht und sie waren keine gesetzgeberische Intention.

Das LG entschied aber, dass es sich bei der Nutzung der festgestellten Fingerabdrücke für Zwecke des Entsperrens des Mobiltelefons des Beschuldigten um eine „ähnliche Maßnahme" zu den in § 81 StPO vorgesehenen handelt. Es sei zwar sicherlich nicht der „klassische Fall", der dem Gesetzgeber vorgeschwebt habe. Dieser habe die Klausel aber offen formuliert. So „wird erreicht, dass sich der statische Gesetzeswortlaut an den jeweiligen Stand der Technik anpasst". Im Sinne dieses „technikoffenen" Ansatzes komme der Verwendung „der festgestellten Fingerabdrücke zum Entsperren eines Mobiltelefons auch eine Identifizierungsfunktion zu". Die Abnahme und Verwendung von Fingerabdrücken für das Öffnen des Mobiltelefons sei für Zwecke der Durchführung des Strafverfahrens „notwendig und mithin verhältnismäßig": „Insbesondere bleibt das Grundrecht des Beschuldigten auf informationelle Selbstbestimmung hinter dem Interesse der Allgemeinheit an einer effektiven Strafrechtspflege zurück." Damit werde auch die Hürde der Angemessenheit übersprungen. Die Maßnahme sei „geeignet und erforderlich", um Erkenntnisse für

die zu führenden Ermittlungen zu gewinnen.

Das Entsperren des Speichermediums sei „ein notwendiges Zwischenziel“. Der Zugriff auf die auf dem Mobiltelefon gespeicherten Daten könne in der Regel „mit ähnlicher Begründung“ auf andere Normen wie etwa § 110 StPO gestützt werden. Die Maßnahme sei auch deswegen erforderlich, weil der Beschuldigte den Code nicht freiwillig herausgegeben habe und etwaige Passwörter nicht auffindbar gewesen seien.

Der auf Straf- und IT-Recht spezialisierte Rechtsanwalt Jens Ferner kritisiert die Entscheidung als „mutlos“ und „ein Stück weit traurig“. Es handle sich um das „übliche Ergebnis, das entsteht, wenn man ergebnisorientiert ‚argumentiert‘“. Dabei sei besonders problematisch, dass „Zufallsfunde“ möglich seien. Wenn Ermittler also wegen Verdachts auf Drogenhandel ein Handy durchsuchen und verbotene andere Inhalte finden, gebe es das nächste Strafverfahren. Das Smartphone als „ausgelagertes Gehirn“ stehe dabei „vollständig zur Verfügung, das gesamte Leben wird durch Strafverfolger untersucht“. Die Richter hätten „wesentliche Literatur“ außen vorgelassen und nicht hinreichend abgewogen. Damit würde das LG „vollkommen Dimension und Tragweite derartiger Entscheidungen“ verkennen: „Der Fingerabdruck ist der Anfang – wie will man damit umgehen, wenn das Smartphone vor das Gesicht gehalten wird und die Person nicht mitwirkt und Grimassen zieht?“ Vielen sei nicht klar, dass hier ein Widerstand gegen Vollstreckungsbeamte drohe. Damit wiederum nähme die grundrechtliche Debatte ganz neu Fahrt auf. Er vermutet, dass die Maßnahme „Schule machen“ wird.

Dies befürchtet auch Rechtsanwalt Udo Vetter: Künftig werde man bei einem Polizeikontakt wohl nicht nur seinen Ausweis zeigen, sondern je nach Gesprächsverlauf auch noch seinen Fingerabdruck hergeben, damit die Beamten „mal auf das Handy schauen können“. Dies fange schon „bei der durch andere Urteile entfachten Jagd auf Blitzer-Apps an“. Dabei sei zu bedenken, dass die Abnahme von Fingerabdrücken nicht unter Richtervorbehalt steht. Beide Anwälte raten daher jegliche biometrische Entschlüsselung zu deaktivieren (Krempl, Polizei entsperrt Smartphone: Landgericht billigt erzwungenen Fingerabdruck, www.heise.de 11.03.2023, Kurzlink: https://heise.de/-7542934; Entsperren Mobiltelefon, Fingerabdruck, zwangsweise Abnahme, Zulässigkeit, https://www.burhoff.de/asp_weitere_beschluesse/inhalte/7646.htm).

AG Trier

Kein Beweisverwertungsverbot beim Handy-Blitzer ohne Rechtsgrundlage

Das Amtsgericht Trier wies mit Urteilen vom 02.03.2023 Einsprüche von drei Autofahrern gegen Bußgeldbescheide wegen Nutzung eines Mobiltelefons am Lenkrad zurück. Zwar stellte das Gericht fest, dass es bisher keine Rechtsgrundlage für den Einsatz des neuen Geräts gibt. Dennoch dürften die vorgelegten Beweise für unerlaubte Handy-Nutzung am Steuer vom Gericht verwertet werden. Rheinland-Pfalz hatte als erstes Bundesland den „Handy-Blitzer“ seit Juni 2022 jeweils drei Monate lang zunächst in Trier und dann in Mainz getestet. Das in den Niederlanden entwickelte System sieht einem normalen Tempo-Blitzer ähnlich. Von einer Autobahnbrücke aus werden zunächst alle vorbeifahrenden Fahrzeuge per Video aufgenommen. Gespeichert werden die Bilder aber erst, wenn die Auswertungssoftware ein Handy und eine typische Handhaltung für Handynutzung beim Fahrer oder der Fahrerin erkannte.

Der Verkehrsrechtler Jürgen Verheul, der zwei Betroffene vertritt, kündigte an beim Oberlandesgericht Koblenz Beschwerde einzulegen: „Das ist eine Ermessensfrage, aber ich finde das nicht konsequent.“ Das rheinland-pfälzische Innenministerium hatte zuvor erklärt, für eine dauerhafte Nutzung sei zweifellos eine „spezifische Rechtsgrundlage“ nötig. Für den Pilotversuch könne man jedoch auf eine Generalklausel im Polizei- und Ordnungsbehördengesetz des Landes zur Gefahrenabwehr zurückgreifen.

Dies sah der Trierer Amtsrichter David Geisen-Krischel anders: „Der Einsatz kann nicht auf die Generalklausel gestützt werden.“ Es gebe „keine ausreichende gesetzliche Grundlage für die Maßnahme“. Auch bei einem Pilotprojekt könne nicht auf eine Ermächtigungsgrundlage verzichtet werden, zumal schon in der Versuchsphase Bußgeldbescheide ergangen seien. Trotz fehlender Rechtsnorm dürften die gesammelten Beweise dennoch verwertet werden, weil die rechtliche „Eingriffsintensität“ nicht so hoch sei. Es gebe vielmehr ein erhebliches öffentliches Interesse an der Sanktionierung der Handy-Nutzung am Lenkrad.

Verheul monierte, das Gericht habe „eindeutig zum Ausdruck gebracht, dass diese Maßnahme eigentlich gar nicht hätte stattfinden dürfen“, aber kein Beweisverwertungsverbot ausgesprochen. Mit dem Einsatz des „Handy-Blitzers“ ohne Rechtsgrundlage werde das Recht auf informationelle Selbstbestimmung verletzt. Auch bei einem Probebetrieb müssten die rechtlichen Grundlagen vorhanden sein, wenn es Sanktionen gebe. In einem vierten Fall gab es einen Freispruch, weil der Autofahrer argumentierte, er habe kein Handy, sondern sein Blutzuckermessgerät in der Hand gehabt. Ein fünfter Fall wurde wegen fehlender Unterlagen vertagt. Alleine auf der Autobahn 602 in Kenn bei Trier sind nach Polizeiangaben 327 Autofahrer mit dem Handy in der Hand erwischt worden. Und haben 100 Euro Bußgeld und einen Punkt in Flensburg auferlegt bekommen. Wie viele Bußgeldbescheide im Laufe des sechsmonatigen Einsatzes des „Handy-Blitzers“ insgesamt ausgestellt wurden, wollte das Ministerium trotz mehrfacher Anfrage nicht mitteilen. Das Innenministerium werde eine Bilanz zum Pilotprojekt präsentieren, hieß es.

Der Allgemeine Deutsche Automobil-Club (ADAC) kritisierte die Entscheidungen des Amtsgerichts Trier. Es sei nicht in Ordnung, dass die Autofahrer die Bußgeldbescheide zahlen müssten. Denn für die Aufzeichnung der Autofahrer durch ein Kamerasystem fehle die gesetzliche Grundlage und es werde in die Persönlichkeitsrechte der Autofahrer eingegriffen. Damit dürften auch die Fotos nicht verwendet werden. Der Datenschutzbeauftragte des Landes Rheinland-Pfalz, Dieter Kugelmann, sieht das ähnlich. Der Jurist

bemängelte bereits im Juni 2022, dass aus seiner Sicht keine Rechtsgrundlage für das Modellprojekt gegeben sei. Eine Aufnahme ohne eine gesetzliche Basis sei nach der Rechtsprechung des Bundesverfassungsgerichts ein Eingriff ins Persönlichkeitsrecht, so Kugelmann (Handy am Steuer: Bußgeldbescheide gegen mit Monocam gefundene Autofahrer gültig, www.heise.de 02.03.2023, Kurzlink: https://heise.de/-7533729; Storr, Trierer Gericht: Bußgeldbescheide wegen „Handy-Blitzern" bleiben gültig, www.swr.de 03.03.2023).

Buchbesprechungen



Kühling, Jürgen (Hrsg.)
BStatG – Bundesstatistikgesetz – Kommentar
C.H.Beck München 2023
ISBN 978 3 406 79857 3, 346 S.,
€ 119,00

(tw) Zu den bisher unterbelichteten Themen des Datenschutzes gehört das Statistikrecht. Zwar war die Aufregung groß und wird immer wieder neu belebt bei der Planung einer Volkszählung oder eines Mikrozensus, womit personenbezogene Daten für statistische Zwecke erhoben werden. Das Volkszählungsurteil aus dem Jahr 1983 ist weiterhin die zentrale Grundlage für unser modernes Verständnis von Datenschutz, auch wenn es in den letzten 40 Jahren viele Fortschreibungen und Weiterentwicklungen gegeben hat. Fortschreibungen und Weiterentwicklungen waren und sind aber beim Statistikrecht rar, obwohl auch die Statistikämter des Bundes und der Länder den technischen Entwicklungen folgten und diese für ihre Arbeit nutzen. Doch blieb das Statistikrecht in Deutschland über 40 Jahre ein Nischenthema; die vorherige Kommentierung des Bundesstatistikgesetzes (BStatG) ist 35 Jahre alt. Die Statistikrechtler blieben unter sich. Und das BStatG blieb in dieser Zeit in Grundstruktur und Inhalt weitgehend unverändert.

Dies ist ein Anachronismus, wenn Statistik die zentrale Erkenntnisquelle für politische Planung sein soll. Überall fallen Daten an, die von statistischer Relevanz sind – sein könnten. Die Datenschutz-Grundverordnung (DSGVO) sieht für die Statistik – gemeinsam mit der Forschung und dem Archivwesen – eine Privilegierung vor. Die Europäische Union mit ihren eigenen Informationsbedarfen macht die nationale Statistik zum Datenzwischenlieferanten. Die Rechtsgrundlagen haben diese Änderungen nur eingeschränkt nachvollzogen – mal abgesehen davon, dass aus der Vollerhebung bei der Volkszählung eine Teilerhebung kombiniert mit einer Registerauswertung wurde.

Es ist also an der Zeit, um zumindest den aktuellen Stand der Statistikverwaltung selbst zu erheben. Und dies gelingt dem Herausgeber Jürgen Kühling und seinen Autorinnen und Autoren. Vorab eine eher formale Kritik: Es ist wünschenswert zu erfahren, welchen beruflichen Hintergrund die Autorenschaft eines juristischen Kommentars hat, da dies inhaltliche Positionen verständlicher machen kann. Dieser Service wird hier unterlassen, so dass nur vermutet werden kann, dass das Interesse am Thema der Lehrstuhlangehörigkeit oder der Zugehörigkeit zu einem Statistikamt zuzuschreiben ist.

Der Inhalt ist überzeugend: Die Paragrafen werden umfassend und mit der nötigen Tiefe besprochen – unter Heranziehung der verfügbaren Literatur und Rechtsprechung und unter Beschreibung der historischen Entwicklungen, verfassungs- und europarechtlichen Vorgaben und praktischen Umsetzungsfragen unter Angabe der Quellen und mit Verweisen innerhalb des Werks. D.h. für die wenigen Menschen, die mit dem Statistikrecht täglich zu tun haben, wird dieser Kommentar umgehend zur zentralen Informationsquelle, mit der viele wesentliche Fragen zwischen zwei Buchdeckeln beantwortet werden. Dies gilt nicht nur für das allgemeine Statistikrecht des Bundes, sondern auch in einem gewissen Maße für das Recht der Spezialerhebungen und das der Länder mit ihrem eigenen Statistikrecht. Die DSGVO findet umfassend Berücksichtigung.

Erfreulich ist auch, dass das Werk sich nicht auf die Wiedergabe der bestehenden Rechtssituation beschränkt, sondern das Recht an den praktischen Herausforderungen misst und dabei immer wieder Defizite feststellt, die letztlich nur durch die Politik behoben werden können. Bisher wird das Statistikrecht von einem strengen Gesetzesvorbehalt geprägt, was zwangsläufig zu einer beschränkten Anpassungsfähigkeit bei Fragestellungen, Datenquellen und Auswertungsmöglichkeiten und damit zu einer Reduzierung des statistischen Erkenntnispotenzials führt. Die private Markt- und Meinungsforschung ist so zum für die Politik handlungsleitenden Instrument geworden, was als Funktion eigentlich der Statistik zukommen sollte. Eine erhöhte Flexibilisierung im Recht und eine engere Verbindung von Statistik und wissenschaftlicher Forschung täte allen Seiten gut. Die Angst, dadurch umfassend ausspioniert zu werden, die den Widerstand gegen die Volkszählungen in den 80er Jahren beförderte, ist Schnee von gestern.

Die Statistik hat ihren Grundrechtstest nach dem Volkszählungsurteil 1983 immer wieder bestanden. Die weiterhin berechtigte Angst geht inzwischen von ganz anderen – privaten wie öffentlichen – Playern aus. Zugleich sollte die Politik erkennen, dass ihr Gerede von der Digitalisierung es dringend nahelegt das Statistikrecht auf den Stand von Technik und Wissenschaft zu heben. Auch insofern dient dieser Kommentar als valide Grundlage.



Knüppel, Kai-Niklas
Datenfinanzierte Apps als Gegenstand des Datenschutzrechts
Internetrecht und Digitale Gesellschaft
Band 38
Duncker & Humblot, Berlin 2022
ISBN 978-3-428-18665-5, 417 S.,
€ 109,90

(tw) Im Internet ist vieles nur scheinbar unentgeltlich – der Nutzer bezahlt mit seinen Daten. Dieser Befund, der inzwischen zumindest bei den etwas bewussteren Internet-Usern angekommen ist, hat praktische und rechtliche Implikationen. Mit den Implikationen für den Datenschutz befasst sich die Doktorarbeit von Kai-Niklas Knüppel äußerst differenziert und ausführlich. Es geht um die Frage, ob, unter welchen Voraussetzungen und in welcher Form App-Anbieter ihr Angebot mit erlangten Daten und deren Nutzung refinanzieren dürfen. Dem Autor geht es nicht nur um die großen Plattformen-Anbieter; er hat vor allem App-Anbieter im Blick, die mit nicht kostenpflichtigen Apps und den dabei erlangten Daten ein valides Geschäftsmodell entwickeln wollen. Seine Grundannahme ist richtig: Solche Apps können mit dem Datenschutz in Einklang gebracht werden. Seine implizite Diagnose ist, dass die aktuelle Praxis mit dem existierenden Datenschutzrecht – das im Prinzip einen gerechten Ausgleich zwischen Betreiber und Nutzerinteressen ermöglicht – oft nicht im Einklang steht. Dieser Befund wird nicht an Beispielen ausdrücklich dargelegt, er ergibt sich für den Leser, wenn er die detailliert dargestellten Anforderungen mit der gelebten Realität vergleicht. Diese Anforderungen werden ausführlich und mit Tiefgang erörtert unter Hinzuziehung der relevanten aktuellen Literatur: Knüppel prüft die Datenschutzvorgaben für datenfinanzierte Apps nach (fast) allen Gesichtspunkten: Datenminimierung, Verantwortlichkeit, Transparenz, Zweckbindung. Den Fokus legt er – zu Recht – auf das Thema Rechtmäßigkeit: Während in den Frühzeiten des Internets vorrangig mit der Einwilligung hantiert wurde, weist er darauf hin, dass die Verarbeitung datenfinanzierter Apps weitgehend vertraglich legitimiert werden muss und kann. Der Einwilligung – die mit allen Konsequenzen widerrufbar sein muss – misst der Autor aber weiterhin eine wichtige Bedeutung bei. Und er widmet sich im Detail der dann zwangsläufigen Frage, wie das Koppelungsverbot in Art 7 Abs. 4 DSGVO anzuwenden ist.

Als Anwendungsfälle nutzt er zwei fiktive Apps, eine zur Navigation und einen Messenger. An diesen Beispielen stellt er seine Bewertungen dar. Beim Durchdeklinieren der rechtlichen Anforderungen behandelt er vier Verarbeitungsphasen: die Sofortnutzung der Daten (I), die Speicherung mit späterer Eigennutzung (II), die Weiternutzung im Konzern (IIIa) und die Weiternutzung durch sonstige Dritte (IIIb); der Autor spricht dabei verkürzend nur von der „Offenlegung" gegenüber Dritten. Er blendet damit argumentativ die Details der Weiternutzung aus und fasst diese unter dem Buzzword „Big Data" zusammen. Er kommt zu dem Ergebnis, dass die Hauptprobleme für den Datenschutz bei den Verarbeitungskategorien III bestehen. Hier fallen dann aber leider die Antworten des Autors eher generisch aus nach dem Muster: je komplexer die Verarbeitung wird, umso höher liegt die Zulässigkeitsschwelle. Zwar zitiert er dann Schwellen, wie sie in Einzelfällen von Literatur und Rechtsprechung behandelt wurden, und er liefert sämtliche Argumente auf einer abstrakten Ebene. Doch was dies dann konkret und praktisch bedeutet, überlässt er dem geneigten Leser.

Dies liegt wohl am verfolgten Konzept des Buchs. Im Eingangskapitel beschreibt Knüppel anschaulich Anwendungsfälle. Doch dann stellt er den Leser vor eine Geduldsprobe – wie dies bei Doktorarbeiten oft der Fall ist: Über knapp 200 Seiten werden allgemein die Grundsätze des Datenschutzes referiert – was man inzwischen tausendfach nachlesen kann – mit nur kurzen Bezugnahmen auf datenfinanzierte Apps. Erst in der zweiten Hälfte des Buchs wird es konkreter. Doch auch hier bleibt vieles generisch und abstrakt: Bzgl. der Verarbeitungskategorien III verharrt die Argumentation im Vagen und in der Rechtsdogmatik, obwohl sich genau hier Pandoras Büchse des Datenmissbrauchs öffnet. Das Thema der sensiblen bzw. sensitiven Daten (Art. 9 DSGVO) wird praktisch überhaupt nicht behandelt – als hätte es Cambridge Analytica nicht gegeben, als würden nicht die großen Plattformen versuchen den Markt der Gesundheits-Apps zu dominieren. Werbung ist nicht gleich Werbung, wenn es um die Eingriffstiefe für die Betroffenen geht. Die Eingriffstiefe ist für das Ergebnis der letztlich nötigen Interessenabwägung entscheidend.

Abschließend werden rechtspolitische Überlegungen angestellt, die richtig zu dem Ergebnis kommen, dass die bestehenden materiell-rechtlichen Vorgaben ausreichend sind, dass aber in Sachen Transparenz einiges an Verbesserungen möglich ist. Nicht angesprochen werden prozessuale Entwicklungen und Möglichkeiten, die darauf hinauslaufen über kollektivrechtlichen Rechtsschutz des Verbraucherrechts oder über Zertifikate die Umsetzungsdefizite zu verringern.

Diese Kritik soll die Verdienste des Buchs nicht schmälern: Knüppel beschreibt die wesentlichen datenschutzrechtlichen Erwägungen zu datenfinanzierten Apps. Die Darstellung ist auf dem neuesten Stand und wertet die relevanten rechtlichen Quellen aus, behandelt die Bezüge zum neuen TTDSG, zum Kartellrecht und zur Richtlinie (EU)

2019/770 mit ihrer zivilrechtlichen Regulierung digitaler Inhalte und Dienste. Das Werk bleibt trotz seiner stark dogmatischen Ausrichtung gut verständlich und ist gut nachvollziehbar. Eine klare Gliederung mit aussagekräftigen Überschriften erleichtert die selektive Nutzung, was jedoch vom sehr knappen Stichwortverzeichnis nur eingeschränkt gesagt werden kann. Das Buch ist eine Fundgrube für jemanden, der sich mit datenfinanzierten Apps wissenschaftlich befasst. Für die Übersetzung in die gelebte Wirklichkeit gibt es viele Anregungen. Antworten auf ganz konkrete Fragen müssen die Datenschützer, App-Entwickler, Verbraucherschützer und sonstige Anwender aber selbst finden.



Christian-Henner Hentsch, Felix Falk (Hrsg.)
Games und Recht – Praxishandbuch
Nomos Verlagsgesellschaft, Baden-Baden 2023
ISBN 978-3-8487-8162-1, 560 S.,
€ 99,00

(ha) Schon das Vorwort dieses 560 Seiten starken Praxishandbuchs „Games und Recht" konstatiert: „Die Games-Branche ist seit Jahren die am dynamischsten wachsende Medienbranche". Dies schlägt sich in der Tat auch in der DANA nieder. Erstmalig erfolgte eine Buchbesprechung zum Thema eSport in der DANA 1/2021 (Dieter Frey, eSport und Recht). In Heft 3/2022 wurde dann der Handkommentar zum Glücksspielrecht von Hamacher/Krings/Otto besprochen. Die beiden Herausgeber des vorliegenden Praxishandbuchs, Christian-Henner Hentsch und Felix Falk, konnten 36 Autoren und Autorinnen aus juristischer Praxis und aus der Forschung gewinnen, um das Thema Spiele so umfassend wie eben möglich abzudecken. Alle Stadien eines Spiels werden in den 31 Kapiteln behandelt: Games-Entwicklung und Publishing, Vertrieb und Marketing und auch die Betrachtung von Plattformen finden ihren Platz. Dabei ist der Stand mit April 2022 vor allem auch durch Beachtung anstehender Regulierungen auf EU- und Bundesebene durchaus aktuell.

Um das an dieser Stelle relevante Thema des Datenschutzes zu bewerten, muss nicht einmal das umfangreiche Stichwortverzeichnis herangezogen werden, denn es gibt ein eigenes Kapitel „Besonderheiten für Games im Datenschutz". Verantwortet wird es von Axel von Walter, Münchener Fachanwalt für Informationstechnologierecht. Seine praxisbezogene Sichtweise ermöglicht auch Ungeübten ein gutes Verständnis der Problematik. Beispielsweise wird vertiefend auf die Problematik der Auskunftsbeschränkung im Bereich der Cheat-Abwehr oder im Beschwerdesystem eingegangen. Unter anderem unter Bezugnahme auf die Veröffentlichung des ULD (Datenschutz in Online-Spielen) werden Best-Practice-Beispiele aufgezeigt für User-Accounts, Social-Gaming, Beschwerdesysteme, Bestenlisten, Chats, Werbung im Spiel, Altersverifikation, Suchtprävention, Anti-Cheat und Virtual Reality. Erfreulich sind besonders die abschließenden, aktuellen Betrachtungen zum TTDSG, zu internationalen Datentransfers sowie zum Einsatz von künstlicher Intelligenz.

Alle Kapitel werden eingeleitet mit einer teils sehr ausführlichen Literaturliste, die nicht nur bei der Betrachtung von Games als Wirtschaftsfaktor und dem Games-Standort Deutschland, sondern auch in den weiteren Kapiteln zu den rechtlichen Fragen durchaus zur Vertiefung geeignet ist. Weitere Bezüge zum Datenschutz werden in den einzelnen Kapiteln zumindest hergestellt, wenn auch nicht immer ausführlich behandelt. So stellt der Herausgeber C.H. Hentsch in einem „Ausblick" lediglich fest: „Höchst fraglich ist auch, ob es aus der DSGVO ein Recht auf Portabilität gibt Spielstände und Charaktere bei einem Anbieterwechsel mitnehmen zu können". Beim Unterkapitel „Vertragsabschluss" weisen andererseits Martin Sester und Anna Kastner erfreulicherweise darauf hin, dass bei der Registrierung die „vom Verbraucher geforderten Daten" dem Prinzip der Datenminimierung unterliegen. Alles in Allem liegt hier ein Praxishandbuch vor, das seinem Namen gerecht wird und das allen Beteiligten an Games-Projekten empfohlen werden kann.



Stephan Hansen-Oest
Datenschutzbeauftragte, Einsteigerlektüre für Anfänger
Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt/Main 2020
ISBN 978-3-8005-0013-0, 316 S.,
€ 39,90

(ha) Es ist immer wieder ähnlich, wenn ein Buch besprochen werden soll: Wie in einer persönlichen Begegnung zählt der erste Eindruck! Beim vorliegenden Softcover-Band aus dem Deutschen Fachverlag ist das nicht nur die Haptik (gut, solide gemacht!), sondern auch die Seitengestaltung (warum ist auf jeder einzelnen Seite der Name des Autors abgedruckt?) und ein Blick in einzelne Kapitel (oh, ich werde geduzt, also: Buch erst einmal weglegen ...).

Zwei Jahre lag das Buch unten im Stapel der Rezensionsexemplare bis die Pflicht siegte und bei solch einem ersten Eindruck bleibt dem Rezensenten nichts anderes, als nochmal von vorne zu beginnen. Da werde ich dann auch gleich im Vorwort aufgeklärt, dass der Rechtsanwalt Stephan Hansen-Oest in 10 Jahren der „Vermittlung von ‚Datenschutzwissen'" die Erfahrung gemacht hat, ich könne die Inhalte auf diese Weise besser verinnerlichen. Nun ja, Stephan, dann duzen wir uns halt.

Allerdings taucht gleich die Frage auf, warum du dein Datenschutzwissen in Anführungszeichen setzt. Apropos Anführungszeichen: Diese sind in den 300 Seiten dermaßen weit verbreitet, dass sich der Sinn vielleicht einer Verlags-Lektorin, nicht aber unbedingt jedem Leser erschließt. Üblicherweise ist das Anführungszeichen ein Mittel, um Zitate zu kennzeichnen. Das erübrigt sich in dieser „Einsteigerlektüre für Anfänger", denn Stephan hat sich nicht die Mühe gemacht irgendeine Quelle anzugeben – ein Literaturverzeichnis fehlt ebenso wie eine Stichwortliste.

Dafür zeigt das Inhaltsverzeichnis, wie locker doch der Datenschutz nach der „Gemüse-Norm" der DSGVO gehandhabt werden kann: So trägt Art. 6 Abs. 1 lit. d den Titel „Dead" und Art. 6 Abs. 1 lit. e wird zu „Echt jetzt". Wie es dazu kommt, erklärt Stephan dann wirklich (Spoiler: „hat mit einer privaten Begebenheit zu tun"), doch der Autor verstärkt am Ende des Kapitels zu Art. 6 Abs. 1 lit. e den Wunsch des Lesers nach einem Stichwortverzeichnis, wenn er dort auf ein Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO hinweist, ohne im vertiefenden Kapitel 12 oder in einer anderen Kapitel-Überschrift diesen Artikel überhaupt zu erwähnen. Das Widerspruchsrecht wird lediglich in Kapitel 21 unter den weiteren Betroffenenrechten aufgezählt.

Aus Sicht des Rezensenten scheint für das Arbeiten mit dieser Einsteigerlektüre neben der DSGVO ein weiterer Gesetzes-Kommentar unumgänglich. Beispielsweise hilft die Definition des Begriffs Dateisystem in Art. 4 Nr. 6 DSGVO nämlich, so Stephan, „nur bedingt weiter". Statt jetzt also den angehenden Datenschutzbeauftragten erklärend zu helfen, belässt es der Autor bei der Aussage: „Die Wahrheit ist derzeit, dass niemand exakt sagen kann, wann nun ein Dateisystem vorliegt oder nicht." Durchaus brauchbar scheint das 40-seitige Kapitel über das Verarbeitungsverzeichnis, das über 20 Verarbeitungen in einem kleinen Unternehmen auflistet und jeweils im selben Stil die verschiedenen Punkte listet. Bei der „Übermittlung von personenbezogenen Daten in ein Drittland" überwiegt dabei die Antwort „keine". Dem Alter des Buchs ist sicher zuzuschreiben, dass bei der Verarbeitung „Internetseite" die Einbindung von Google Webfonts durch die „Teilnahme von Google am Privacy Shield" als angemessen bezeichnet wird.

Das Buch endet schließlich nach einem gut 50 Seiten umfassenden Kapitel „Wir bauen uns ein Datenschutzmanagementsystem" mit dem Schlusswort. Hier empfiehlt mir Stephan, wenn der „Stoff" mich zu erschlagen scheine mich „einmal durchzuschütteln", mich „darauf zu besinnen, dass es Sinn macht, Stück für Stück vorzugehen" und mich nach der „Zwiebeltheorie" „Schale für Schale tiefer in die Details" einzuarbeiten. Das Durchschütteln habe ich mir erspart und bin auch nicht weiter in die Details eingestiegen.



Schmidbauer, Wilhelm/Steiner, Udo
Polizeiaufgabengesetz – Polizeiorganisationsgesetz
Kommentar
C.H.Beck-Verlag München, 6. Aufl. 2023
ISBN 978 3 406 79809 2, 1.291 S.,
€ 69,00

(tw) Während sich das Polizeirecht bzw. generell das Sicherheitsrecht in den 90er Jahren im Zentrum der datenschutzrechtlichen Diskussion in Deutschland befand, spielt es inzwischen nur noch eine Rolle unter vielen und findet in der politischen Diskussion nicht mehr die frühere hitzige und kontroverse Resonanz. Ein Grund hierfür mögen die vielen Entscheidungen des Bundesverfassungsgerichts (BVerfG) hierzu gewesen sein, jüngst ergänzt durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH). Beide Gerichte mussten immer wieder Gesetzgebungsakte im Sicherheitsrecht als europa- bzw. verfassungsrechtswidrig verwerfen, was zum einen zu einer Einhegung der Sicherheitsbehörden, namentlich der Polizei, führte, zum anderen deren Akzeptanz in der Öffentlichkeit, selbst der außerparlamentarischen Opposition, stärkte. Das Recht der Polizei wie deren Praxis ist rechtsstaatlich stark eingehegt, so dass Auswüchse, wie sie z.B. in den USA bekannt werden, eher die Ausnahme als die strukturelle Regel sind.

Dem dienen auch das ausdifferenzierte Polizeirecht und im Hinblick auf informationelle Maßnahmen die dort zu findenden spezifischen Datenverarbeitungsregeln.

Bei aller verfassungsrechtlichen Einhegung gibt es in Deutschland erhebliche Unterschiede im Polizeirecht, das zu den originären Landeszuständigkeiten gehört. Und es hat Tradition, dass die Südländer einen eher konservativen eingriffsfreundlichen Kurs verfolgen, während im Norden eher eine liberale, eingriffskritische Praxis besteht. Insofern ist der Polizeirechtskommentar von Schmidbauer/Steiner aufschlussreich. Schmidbauer ist altgedienter Polizist, zuletzt bis Februar 2022 Landespolizeipräsident Bayerns. Steiner war Richter am BVerfG. Er kommentiert in dem über 1.200 Seiten dicken Werk lediglich 45 Seiten zur polizeirechtlichen Verantwortlichkeit. Es ist beeindruckend, wie der Hauptautor die umfangreiche Materie bearbeitet und dabei sowohl die Ebenen des Bundes-, des Verfassungs- wie des Europarechts mit behandelt.

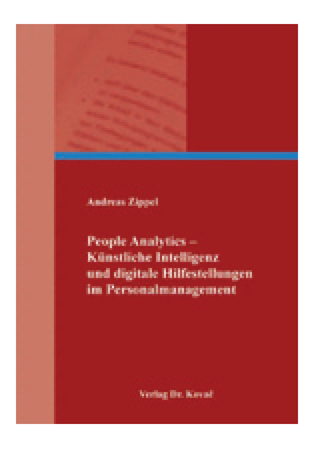
Schon in den Vorworten macht Schmidbauer seine Grundhaltung klar: Er sieht nicht nur die Bürger als Betroffene staatlicher Gewaltanwendung, sondern auch als Opfer von Straftätern und Gefährdern, denen die Polizei Freund und Helfer ist. Damit liegt er auf der Linie der bayerischen Politik, die Befugnisbeschränkungen für die Polizei eher kritisch sieht und Befugniserweiterungen zwecks Herstellung von Sicherheit und Ordnung begrüßt und fordert. Dessen ungeachtet referiert Schmidbauer die Anforderungen des BVerfGs und trägt diese weitgehend mit, was ihn aber nicht daran hindert zugleich kritisch argumentierend Stellung zu beziehen und zu relativieren. So vertritt er z.B. mit der ganz herrschenden Meinung, dass auch aus bayerischem Verfassungsrecht kein subjektives Recht auf Sicherheit abge-

leitet werden kann, wenngleich er aber seine Sympathie für ein solches Instrument nicht verbirgt und beklagt, dass dem Verfassungsprinzip der Gewährleistungspflicht der inneren Sicherheit zu wenig Aufmerksamkeit geschenkt wird.

Er hält die Doppeltürargumentation des BVerfGs für falsch, wonach es für eine Datenbeschaffung nicht nur eines Erhebungsrechts der Polizei, sondern auch eines Übermittlungsrechts der Datenquelle bedarf. Die Begrenzungen des Datenaustauschs zwischen Geheimdiensten und Polizei sieht er kritisch. Der Begriff der drohenden Gefahr als polizeiliche Eingriffsschwelle ist für ihn kein Grundrechtsproblem.

Diesen Positionen mag man nicht zustimmen, doch muss man sich mit ihnen auseinandersetzen, was hier gelingt, weil Schmidbauer nicht nur Schlagworte verbreitet, sondern praktisch argumentiert und Bereitschaft zum rechtlichen Diskurs signalisiert.

Der Diskurs kommt dann aber oft in dem gewaltigen Werk etwas zu kurz, beschränkt sich der Autor doch vor allem auf die bayerische Debatte und berücksichtigt eher wählerisch die Literatur aus dem Rest der Republik. Für die affirmative Auslegung des Polizeiaufgabengesetzes und des Polizeiordnungsgesetzes des Freistaates ist das Buch in jedem Fall eine valide Quelle, nicht aber für eine verfassungsrechtliche oder gar verfassungspolitisch kritische Hinterfragung. Insofern mag die inhaltliche Beschränkung für die Nutzung dieses „Standardwerks" für die Ausbildung in Bayern ausreichend sein. Sie hat aber zur Folge, dass für die wissenschaftliche Behandlung polizeirechtlicher Fragen weitere Quellen herangezogen werden müssen. Und bzgl. der Polizeipraxis gibt es Defizite, da die Schnittstellen der polizeilichen Gefahrenabwehr, sogar mit der Strafverfolgung, aber insbesondere mit den praxisrelevanten Fragen der Kooperation mit Nachrichtendiensten oder gemäß dem Ausländerrecht, nur am Rande erwähnt werden. Auch etwas selektiv sind das Stichwort- und das Abkürzungsverzeichnis, was bei manchen Fragestellungen ein längeres Suchen oder zumindest für weniger geschulte Leser ergänzende Recherchen im Internet nötig macht. Angesichts des Umfangs des Werkes wundert es auch nicht, dass der Autor weniger wichtige aktuelle Entwicklungen ab und zu nicht berücksichtigt. Dies ändert nichts an der Seriosität des Kommentars und an seiner Relevanz, zumal dieser die derzeit wohl prominenteste konservative Stimme im Polizeirecht in Deutschland wiedergibt.



Zippel, Andreas
People Analytics – Künstliche Intelligenz und digitale Hilfestellungen im Personalmanagement
Verlag Dr. Kovac, Hamburg 2023
ISBN 978-3-339-13428-8, 437 S.,
€ 129,80

(tw) Der Einsatz sog. künstlicher Intelligenz (KI) im Beschäftigtenbereich spielt zunehmend in der Praxis eine Rolle. Es geht darum Merkmale von Bewerbenden und Beschäftigten im Personalmanagement zur Effektivierung von Entscheidungsprozessen auszuwerten. Zumeist dienen Instrumente des „People Analytics" noch der Vorbereitung von Personalmaßnahmen, aber insbesondere im Bewerbungs- bzw. Einstellungsprozess übernimmt der Computer zunehmend zumindest die Vorselektion von Stellensuchenden. In der Doktorarbeit von Zippel wird in umfassender Weise aus juristischer Sicht der Algorithmeneinsatz durch Arbeitgeber dargestellt und bewertet, indem die Vielzahl von dazu veröffentlichten Aufsätzen und Kommentierungen sowie die Rechtsprechung zusammenführt werden. Als praktischer Ratgeber für Betriebsräte gibt es schon das „Praxishandbuch Künstliche Intelligenz" von Lothar Schröder und Petra Höfers (2022, Besprechung dazu in DANA 3/2022, 208).

Das Buch beschreibt zunächst die technischen Grundlagen und behandelt am Rande auch, welche Rechte selbst bei nicht-personenbezogenen KI-Trainingsdaten eine Rolle spielen können (Patente, Gebrauchsmuster, Markenangaben und Geschäftsgeheimnisse) und dass wettbewerbs-, zivil- und strafrechtliche Fragen relevant sein können. Das zentrale Thema Zippels ist die Frage der Zulässigkeit der KI-Nutzung von Beschäftigtendaten durch den Arbeitgeber. Im Rahmen der Ausübung von dessen Direktionsrecht kann demnach eine solche Nutzung für Leistungskontrollen oder -verbesserungen, Mitarbeiterförderung und -weiterentwicklung und selbst zur Kündigung zulässig sein, nicht aber für reine KI-Trainingszwecke, da keine Notwendigkeit im Rahmen des Arbeitsvertrags besteht. Mangels Freiwilligkeit hält er – zu Recht – die Einwilligung für untauglich. Kritisch sieht er Betriebsvereinbarungen, wobei er zugesteht, dass darin zugesicherte Instrumente die Angemessenheit eines KI-Einsatzes herstellen können. Der KI-Einsatz unterliegt der Verhältnismäßigkeitskontrolle, wobei die Grundsätze der Transparenz, der Datenminimierung, der Speicherbegrenzung und der Datenrichtigkeit sowie der Verbote von Persönlichkeitsprofilen und von Diskriminierungen zu beachten sind. Das Verbot automatisierter Entscheidungen nach Art. 22 DSGVO wird vom Autor restriktiv ausgelegt; er geht davon aus, dass KI im Beschäftigtenverhältnis regelmäßig noch mit einer qualifizierten Einbindung eines Menschen erfolgt.

Die Arbeit von Zippel ist eine gediegene dogmatische Arbeit zum Thema, die das verfügbare Material gut aufbereitet. Dies erfolgt dann nochmals am Ende der Arbeit in einer übersichtlichen Zusammenfassung. Es ist aber wegen der diskursiven Darstellung der praktischen Bezüge z.B. für Betriebsräte oder auch Personalverantwortliche schwer geplante oder vorzufindende KI-Angebote gemäß den dogmatischen Vorgaben einzuordnen und zu bewerten. Insofern ist die Arbeit ein nützlicher Beitrag in der gerade heiß laufenden KI-Diskussion. Mit dem KI-Act der EU und der Diskussion über die praktische Anwendung von Chatbots, die auch im Arbeitsleben eine Rolle spielen (werden), werden weitere Kapitel zu diesem Thema aufgeschlagen.



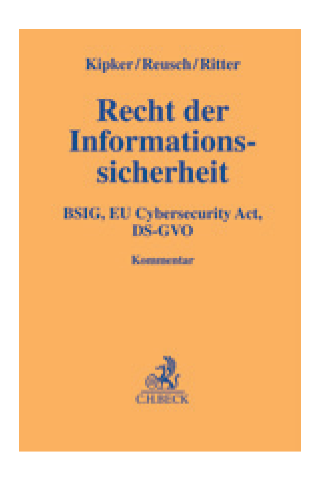
Podszun, Rupprecht
Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks
Nomos Verlagsgesellschaft
Baden-Baden 2023
ISBN 978-3-7560-0521-5 (Print),
116 S., € 34,00
ISBN 978-3-7489-3877-4
(PDF), kostenlos

(ak) Parallel zum Gesetzgebungsvorgang zum neuen EU Data Act legt Rupprecht Podszun unter Mitarbeit von Philipp Offergeld eine Studie vor, die die Anforderungen an den zu regulierenden Datenmarkt aus der Sicht des Handwerks untersucht. Die von den Wirtschaftsministerien des Bundes und der Länder geförderte und von Verbänden des Handwerks unterstützte Arbeit beschreibt die Anforderungen des Handwerks an den Zugang zu Daten in der digital gesteuerten Wirtschaft. Es wird deutlich gemacht, dass mit der zunehmenden Verwendung von smarten Geräten und deren Vernetzung der Zugriff auf die für die Wartung und Reparatur solcher Geräte notwendigen Daten nicht mehr nur durch den Handwerker vor Ort alleine möglich ist, sondern in zunehmendem Maße durch Übermittlung von Geräte-Daten z.B. an den Hersteller erfolgt. Unter Umständen sind Daten vor Ort gar nicht mehr ohne weiteres zugreifbar. Dadurch verändert sich das Verhältnis zwischen dem Handwerksbetrieb und dem Hersteller erheblich. Zum Beispiel kann der Hersteller aufgrund von Daten die Notwendigkeit vorbeugender Wartung erkennen und den Nutzer informieren oder die Wartung selbst veranlassen, um Ausfälle zu vermeiden. Der Handwerksbetrieb ist in einem solchen Szenario auf den Zugang zu den Daten des Herstellers angewiesen, um einen wesentlichen Teil seiner wirtschaftlichen Tätigkeit ausführen zu können. Außer den Geräteherstellern können auch die Betreiber der zur Datenübertragung und Sammlung genutzten Netze und Plattformen privilegierte Positionen in Bezug auf die verfügbaren Daten erlangen. Dass die Kontrolle großer Datenmengen zu Machtpositionen führt, wird mit den Fragestellungen der Verarbeitung personenbezogener Daten vertraute Leser nicht überraschen. Auch durch die Kontrolle nicht personenbezogener Daten können Wettbewerbsverzerrungen und andere Probleme auftreten, die letztendlich auch die Position der Verbraucher in der digitalisierten Wirtschaft schwächen.

Die Studie untersucht anhand verschiedener Szenarien, wie die im Vorschlag der Europäischen Kommission vorgesehenen Regelungen des Data Act auf die Beziehungen zwischen den verschiedenen Akteuren im Datenmarkt wirken können, und macht Empfehlungen, wie deren Wirksamkeit aus Sicht des Handwerks verbessert werden könnte. Die klare Definition und Unterscheidung der verschiedenen Gruppen und ihrer jeweiligen Interessen und Bedürfnisse ist sehr hilfreich bei der Analyse. Insgesamt kommen die Autoren zu 28 Empfehlungen, die von Parlamentariern oder Regierungen in die Verhandlungen zum Data Act eingebracht werden könnten.

Gegenstand der Studie ist auch das Zusammenspiel des vorgesehenen Data Act mit anderen Rechtsgebieten, unter anderem dem Datenschutz. Aus zwei Gründen wird hier relativ wenig Interaktion erwartet. Zum einen ist ein Großteil der betrachteten Datenbestände überhaupt nicht personenbezogen (oder kann ohne Wertverlust anonymisiert werden), zum anderen stellt der Data Act klar, dass die Bestimmungen der DSGVO unberührt bleiben. Insgesamt findet die Studie, dass keine neuen Rechtsunsicherheiten bezüglich der Nutzung personenbezogener Daten durch die Nutzung durch Dritte nach dem Data Act entstehen. Die Autoren weisen darauf hin, dass bei Nutzung eines Geräts durch andere als den Erwerber die Erlangung der datenschutzrechtlichen Einwilligung aller Nutzer schwierig sein kann, erklären aber auch, dass im Gegensatz zur weitverbreiteten Meinung die Einwilligung nicht die alleinige Rechtsgrundlage sein kann, sondern auch die anderen Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO eine Rolle spielen können.

Die klare Definition der betrachteten Zielgruppe und die systematische Analyse der Studie geben Anlass zu dem Wunsch, dass die Verhandler im Gesetzgebungsverfahren die Empfehlungen analysieren und berücksichtigen, und dass der nationale Gesetzgeber die nach Verabschiedung der Verordnung noch notwendigen Regelungen, z.B. die nationalen Durchsetzungsmechanismen, entsprechend effektiv gestaltet.



Kipker, Dennis Kenji/Reusch, Philipp/
Ritter, Steve
Recht der Informationssicherheit
C. H. Beck München 2023
ISBN 978 3 406 78339 5, 1.032 S.,
€ 139,00

(ak) Mit der steigenden Bedeutung der Informationssicherheit durch weiteren Einsatz digitaler Systeme in Wirtschaft und Verwaltung und der immer stärkeren Wahrnehmung von Angriffen auf diese Systeme nehmen auch die Bemühungen der Gesetzgeber zu den rechtlichen Rahmen für die notwendigen Maßnahmen der Betreiber wichtiger Informationssysteme und die öffentlichen Aufgaben in diesem Bereich klarer und umfassender zu gestalten. Damit wird es schwieriger für die Praktiker den Überblick über die gesetzlichen Vorgaben zu behalten. Dies gilt nicht zuletzt, da zusätzlich zu allgemein gül-

tigen Regeln auch besondere Regeln für bestimmte Wirtschaftssektoren gelten.

Der von den Herausgebern Kipker, Reusch und Ritter in Zusammenarbeit mit 18 anderen Autorinnen und Autoren verfasste Kommentar zielt darauf ab die in Deutschland anwendbaren IT-Sicherheitsvorschriften umfassend darzustellen, auch unter Berücksichtigung einiger besonders betroffener Sektoren. Dabei werden sowohl die deutsche Gesetzgebung (BSI-Gesetz, Kritis-V, Teile von Atomgesetz, EnWG, TKG und TTDSG) als auch die unmittelbar anwendbaren EU-Rechtsakte (CSA, Teile der DSGVO) umfassend kommentiert.

Angesichts der Komplexität der Gesetzgebung ist alleine schon die Auswahl der Fundstellen in einer konsolidierten Fassung hilfreich, besonders mit Blick auf die Vielzahl von Änderungen unterschiedlicher Gesetze, wie sie etwa durch das ITSiG 2.0 eingeführt wurden. Auch wenn die ausgewählten Texte alle als relevant angesehen werden können, kann man sich eine klarere Motivation der Auswahl durch die Herausgeber wünschen. In einer späteren Auflage mag eine solche Einführung hinzugefügt werden. Die Klarstellung, warum welche Sektoren berücksichtigt werden, wäre zu begrüßen, auch um Nutzer des Kommentars auf eventuell wichtige weitere Rechtsquellen hinzuweisen, etwa die spezifischen Regelungen für den Finanzsektor.

Im Kontext des Datenschutzes ist besonders zu begrüßen, dass auch die für die Informationssicherheit wichtigen Bestimmungen des TTDSG und der DSGVO berücksichtigt werden. Ein Hinweis auf die entsprechenden Regelungen im BDSG, die der Umsetzung der EU-Richtlinie 2016/680 über den Datenschutz im Polizei- und Sicherheitsbereich dienen, wäre sinnvoll. Die Auswahl der kommentierten Paragraphen des TTDSG erscheint umfassend. Bezüglich der DSGVO überrascht zunächst die Beschränkung auf nur drei Artikel (5, 24 und 32), da ja auch andere Teile der DSGVO für die Durchführung der Sicherheitsmaßnahmen wichtige Bestimmungen enthalten. Allerdings zeigt die umfassende Kommentierung dieser Vorschriften, dass die Autoren mit der großen Bedeutung des Managements und der Durchführung von technischen und organisatorischen Maßnahmen zur IT-Sicherheit für die ordnungsgemäße Verarbeitung personenbezogener Daten vertraut sind. Auch praktische Schritte werden dargestellt.

Da die Verantwortung für die praktische Implementierung von Datenschutz und IT-Sicherheit in vielen Organisationen von enger Zusammenarbeit geprägt ist, ist der vorliegende Kommentar zum Recht der Informationssicherheit auch für Datenschützer eine sinnvolle Ergänzung zur Datenschutzliteratur.













Cartoon

ICH HABE GESTERN GELESEN, DASS SICH DIE SPANISCHE REGIERUNG BEI DEN BERATUNGEN ZUR GEPLANTEN CHATKONTROLLE FÜR EIN VERBOT DER ENDE-ZU-ENDE-VERSCHLÜSSELUNG AUSGESPROCHEN HAT.

AHA – UND WAS KOMMT ALS NÄCHSTES? DAS VERBOT VON TÜRSCHLÖSSERN, DAMIT DIE POLIZEI OHNE HINDERNISSE IN JEDER WOHNUNG NACH BELASTENDEM MATERIAL SUCHEN KANN? VERBOT VON BRIEFUMSCHLÄGEN UND PAKETVERPACKUNGEN?

JEDENFALLS IST ES FÜR HACKER DURCH KLARTEXT-CHATS DEUTLICH LEICHTER INHALTE ZU MANIPULIEREN UND MISSLIEBIGE PERSONEN ZU KOMPROMITTIEREN. POLITIKER SCHEINEN DABEI AUSZUBLENDEN, DASS SIE DADURCH SELBST BETROFFEN SEIN KÖNNEN.

https://www.heise.de/news/Chatkontrolle-Spanien-plaediert-fuer-EU-Verbot-von-Ende-zu-Ende-Verschluesselung-9062428.html